



Customer No. 22,852  
Attorney Docket No. 04329.3293

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: )  
)  
Shinichi KURIHARA et al. )  
) Group Art Unit: 2155  
Application No.: 10/807,313 )  
) Examiner:  
Filed: March 24, 2004 )  
)  
For: CONTENT DELIVERY SERVICE )  
PROVIDING APPARATUS AND )  
CONTENT DELIVERY SERVICE )  
TERMINAL UNIT )

**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, VA 22313-1450**

Sir:

**CLAIM FOR PRIORITY**

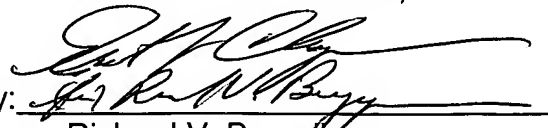
Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 2003-146704, filed May 23, 2003, for the above-identified U.S. patent application.

In support of this claim for priority, enclosed is one certified copy of the priority application.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

Dated: June 17, 2004

By:   
Richard V. Burgujian  
Reg. No. 31,744

RVB/FPD/gah  
Enclosures

ERNEST F. CHAPMAN  
Reg. No. 25,961

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   5 月 2 3 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 1 4 6 7 0 4  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 1 4 6 7 0 4 ]

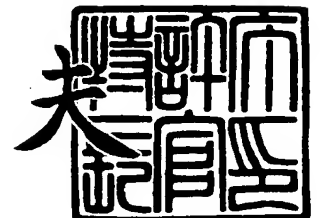
出      願      人            株 式 会 社 東 芝  
Applicant(s):



2 0 0 4 年   4 月   6 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 A000301771

【提出日】 平成15年 5月23日

【あて先】 特許庁長官 殿

【国際特許分類】 H04H 9/00

【発明の名称】 コンテンツ配信サービス提供装置及びコンテンツ配信サービス端末装置

【請求項の数】 17

【発明者】

    【住所又は居所】 東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内

    【氏名】 栗原 伸一

【発明者】

    【住所又は居所】 東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内

    【氏名】 中島 孝次

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100091351

    【弁理士】

    【氏名又は名称】 河野 哲

## 【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

## 【選任した代理人】

【識別番号】 100108855

【弁理士】

【氏名又は名称】 蔵田 昌俊

## 【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

## 【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

## 【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ配信サービス提供装置及びコンテンツ配信サービス端末装置

【特許請求の範囲】

【請求項 1】 少なくとも媒体固有識別子及び媒体鍵情報の媒体情報が書き込まれた情報記憶媒体に、または前記情報記憶媒体がセットされた状態で前記情報記憶媒体とは別の情報記憶媒体にコンテンツを記録可能とするユーザ側の端末装置に対して、通信回線を介してコンテンツの配信サービスを行うコンテンツ配信サービス提供装置であって、

前記配信サービスの加入申請を行うユーザの個人情報、サービス範囲、支払い方法を含むユーザ情報を事前登録し、ユーザ毎にサービス提供時の認証情報の配布、配信コンテンツ選択リストの配布及びコンテンツ選択要求受付、課金・決済を管理するユーザ管理制御装置と、

前記配信サービスを行うコンテンツの著作権保有者または著作権管理者からコンテンツと共にコンテンツ鍵生成条件を取得し、前記コンテンツ鍵生成条件を基にコンテンツ鍵及びこのコンテンツ鍵による暗号化コンテンツを生成する暗号化コンテンツ制御装置と、

前記暗号化コンテンツ制御装置で生成されるコンテンツ鍵を蓄積すると共に、前記情報記憶媒体の媒体情報の全部または一部を登録し、前記ユーザからのコンテンツ要求時に提示される媒体情報または媒体情報及び端末装置固有情報を用いて前記要求コンテンツに対応するコンテンツ鍵を暗号化し、この暗号化コンテンツ鍵を要求元ユーザの端末装置に発行する暗号化コンテンツ鍵制御装置と、

前記暗号化コンテンツ制御装置で生成される暗号化コンテンツを蓄積し、前記ユーザからのコンテンツ要求時に該当する暗号化コンテンツを選択し、要求元ユーザの端末装置に配信するコンテンツ制御配信装置とを具備することを特徴とするコンテンツ配信サービス提供装置。

【請求項 2】 請求項 1 記載のコンテンツ配信サービス提供装置に用いられるユーザ管理制御装置であって、

前記コンテンツ配信サービスの加入申請としてユーザ個人情報、サービス適用

範囲、支払い方法を含むユーザ情報を提示したユーザの適否を判断するユーザ適否判断手段と、

この判断手段で適正と判断された適正ユーザの前記ユーザ情報を管理するユーザ情報管理手段と、

前記ユーザに対してログイン用の認証情報を発行する認証情報発行手段と、

前記認証情報に基づいてログインされたユーザ側の端末装置に対し、前記ユーザ情報管理手段で管理されるユーザ情報のサービス適用範囲から配信可能なコンテンツを選択しそのリストを提供するリスト提供手段と、

前記ユーザ側の端末装置から前記リストに提示されるコンテンツの選択を受けて前記コンテンツ制御配信装置に該当するコンテンツの配信を指示する配信指示手段と、

前記コンテンツの配信時に前記ユーザの課金・決済情報を管理する課金・決済管理手段とを備えることを特徴とするコンテンツ配信サービス提供装置のユーザ管理制御装置。

【請求項 3】 さらに、前記コンテンツの配信を行う際に、前記ユーザ側の端末装置にコンテンツ取得用のアプリケーションを起動するための起動情報を配信する起動情報配信手段を備えることを特徴とする請求項 1 記載のコンテンツ配信サービス提供装置。

【請求項 4】 請求項 1 記載のコンテンツ配信サービス提供装置に用いられる暗号化コンテンツ制御装置であって、

前記コンテンツを指定のデジタル符号化形式でエンコードする、あるいは指定のデジタル符号化形式に変換し、前記コンテンツ鍵生成条件に基づいてコンテンツ鍵を生成し、当該コンテンツ鍵により前記コンテンツを暗号化する暗号化コンテンツ生成手段と、

前記暗号化コンテンツ生成部で暗号化された暗号化コンテンツを前記コンテンツ制御配信装置に発行する暗号化コンテンツ発行手段と、

前記暗号化コンテンツ生成部で生成されたコンテンツ鍵を前記コンテンツ鍵制御装置に発行するコンテンツ鍵発行手段とを具備することを特徴とするコンテンツ配信サービス提供装置の暗号化コンテンツ制御装置。

【請求項 5】 請求項 1 記載のコンテンツ配信サービス提供装置に用いられる暗号化コンテンツ鍵制御装置であって、

前記暗号化コンテンツ制御装置で生成されるコンテンツ鍵を蓄積するコンテンツ鍵蓄積部と、

前記情報記憶媒体の媒体情報の全部または一部を格納する媒体情報格納部と、

前記ユーザからのコンテンツ要求時に、要求コンテンツに対応するコンテンツ鍵を前記コンテンツ鍵蓄積部から読み出し、ユーザから提示される媒体情報に基づいて前記コンテンツ鍵を暗号化する暗号化処理部と、

前記暗号化処理部で生成された暗号化コンテンツ鍵を要求元に発行する暗号化コンテンツ鍵発行部とを具備することを特徴とするコンテンツ配信サービス提供装置の暗号化コンテンツ鍵制御装置。

【請求項 6】 前記暗号化処理部は、前記ユーザから前記媒体情報と共に提示される端末装置固有情報、コンテンツ識別情報、コンテンツ配信制御装置を識別するための情報、媒体連携コンテンツ取得装置を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ鍵個別情報の少なくともいずれかを取得し、これらの情報に基づいて前記コンテンツ鍵の暗号化を行うことを特徴とする請求項 5 記載のコンテンツ配信サービス提供装置の暗号化コンテンツ鍵制御装置。

【請求項 7】 請求項 1 記載のコンテンツ配信サービス提供装置に用いられるコンテンツ制御配信装置であって、

前記暗号コンテンツ制御装置で生成される暗号化コンテンツを蓄積する暗号化コンテンツ蓄積部と、

前記ユーザからのコンテンツ要求時に前記暗号化コンテンツ蓄積部から該当する暗号化コンテンツを読み出し、前記暗号化コンテンツ鍵制御装置で生成される暗号化コンテンツ鍵に基づいて前記暗号化コンテンツを再暗号化する暗号化処理部と、

前記暗号化処理部で生成された暗号化コンテンツを要求元に配信する配信処理部とを具備することを特徴とするコンテンツ配信サービス提供装置のコンテンツ制御配信装置。

【請求項 8】 さらに、前記ユーザ側の端末装置との間で日時情報を同期させる日時情報同期手段を備えることを特徴とする請求項 1 記載のコンテンツ配信サービス提供装置。

【請求項 9】 さらに、前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置にそれぞれ暗号化コンテンツ鍵生成、暗号化コンテンツ配信に、任意のコンテンツ視聴条件、オプション情報を選択的に含めることを特徴とする請求項 1 記載のコンテンツ配信サービス提供装置。

【請求項 10】 請求項 1 記載のコンテンツ配信サービス提供装置から前記コンテンツ配信サービスを受けるコンテンツ配信サービス端末装置であって、

前記ユーザ管理制御装置との間で、前記認証情報に基づくログインを行い、前記配信コンテンツ選択リストに基づいてコンテンツ選択要求を行うユーザアクセス・コンテンツ選択装置と、

前記コンテンツ選択要求時に、前記情報記憶媒体から前記媒体情報を取得して前記コンテンツ配信サービス提供装置に送り、前記コンテンツ配信サービス提供装置から暗号化コンテンツ鍵及び暗号化コンテンツを受け取って、共にまたは別々に前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体の書込可能領域に書き込む媒体連携コンテンツ取得装置と、

前記情報記憶媒体から任意の暗号化コンテンツを読み出すと共に対応する暗号コンテンツ鍵を読み出し、前記暗号化コンテンツ鍵を前記媒体情報に基づいて復号し、復号されたコンテンツ鍵に基づいて暗号化コンテンツを復号するコンテンツ提示制御装置とを具備することを特徴とするコンテンツ配信サービス端末装置。

【請求項 11】 請求項 10 記載のコンテンツ配信サービス端末装置に用いられるユーザアクセス・コンテンツ選択装置であって、

前記ユーザ管理制御装置に予め提示される認証情報に基づいてログインし、要求される情報を提示するログイン手段と、

前記アクセスにより前記ユーザ管理制御装置から提示される配信コンテンツ選択リストを取得して提示し、ユーザ指定のコンテンツ選択要求を前記ユーザ管理制御装置に通知するコンテンツ選択要求手段とを具備することを特徴とするコン



テンツ配信サービス端末装置のユーザアクセス・コンテンツ選択装置。

【請求項 1 2】 請求項 1 0 記載のコンテンツ配信サービス端末装置に用いられる媒体連携コンテンツ取得装置であって、

前記コンテンツ選択要求時に、前記情報記憶媒体から前記媒体情報を取得し、この媒体情報または媒体情報及び端末装置固有情報を前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置に通知する情報通知手段と、

前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置から暗号化コンテンツ鍵及び暗号化コンテンツを受け取り、共にまたは別々に前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体の書込可能領域に書き込む情報記憶手段とを具備することを特徴とするコンテンツ配信サービス端末装置の媒体連携コンテンツ取得装置。

【請求項 1 3】 さらに、前記コンテンツ配信サービス提供装置から配信される起動情報によって起動し、前記コンテンツ配信サービス提供装置との間で相互認証を行い、認証確認後に前記情報通知手段及び情報記憶手段の処理実行を指示する起動手段を備えることを特徴とする請求項 1 2 記載のコンテンツ配信サービス端末装置の媒体連携コンテンツ取得装置。

【請求項 1 4】 さらに、前記コンテンツ配信提供装置から提供される日時情報に基づいて処理を実行する日時情報管理手段を備えることを特徴とする請求項 1 0 記載のコンテンツ配信サービス端末装置。

【請求項 1 5】 前記媒体連携コンテンツ取得装置は、前記コンテンツ配信サービス提供装置からコンテンツ視聴条件を受け取った場合、その視聴条件を前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体に書き込み、

前記コンテンツ提示制御装置は、前記暗号化コンテンツ及び暗号化コンテンツ鍵の復号化の際に、前記コンテンツ視聴条件に基づいて処理を実行することを特徴とする請求項 1 0 記載のコンテンツ配信サービス端末装置。

【請求項 1 6】 前記暗号化コンテンツ視聴条件が視聴期限を指定している場合、前記情報記憶媒体に書き込まれたコンテンツを日時情報により管理し、前記視聴期限の経過時に前記情報記憶媒体から前記コンテンツを使用不能にするこ

とを特徴とする請求項 1 2 記載のコンテンツ配信サービス端末装置の媒体連携コンテンツ取得装置。

【請求項 1 7】 前記媒体情報が書き込まれた情報記憶媒体とは別の情報記憶媒体に前記暗号化コンテンツ、暗号化コンテンツ鍵の少なくともいずれか一方が書き込まれている場合には、前記媒体情報が書き込まれた情報記憶媒体がセットされた状態でのみ前記暗号化コンテンツ及び暗号化コンテンツ鍵の読み出し、復号処理を実行することを特徴とする請求項 1 0 記載のコンテンツ配信サービス端末装置のコンテンツ提示制御装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、ユーザ側の端末装置に対して、通信回線を介してコンテンツの配信サービスを行うコンテンツ配信サービス提供装置と、そのサービスを受けるユーザ側端末装置に係り、特にコンテンツの著作権を保護する技術に関する。

【0 0 0 2】

【従来の技術】

近年、インターネット等の通信技術、デジタル信号処理によるデータ圧縮技術等の発達により、通信回線を利用して、楽曲、映画、ゲーム等の膨大なデータ量のコンテンツを配信することが可能となり、場所、時間を問わず、コンテンツ配信サービスを受けられるようになった。このコンテンツ配信サービスを実現するシステムでは、購入・視聴希望者（以下、ユーザ）がパーソナルコンピュータ（以下、パソコン）あるいはセットトップボックス（STB）等の通信端末機器を通じて所望のコンテンツを配信しているコンテンツ配信センターへアクセスし、メニュー画面に従って購入あるいは視聴要求を通知することで、ダウンロードまたは再生可能とする構成が一般的である。

【0 0 0 3】

但し、現状では、ユーザがセンターにアクセスしても、人気、話題性のあるコンテンツは、コンテンツの紹介、宣伝用コンテンツが提供されるのみで、欲する視聴用の本番コンテンツは、すぐに視聴することが出来ない通信販売によるもの

がほとんどである。理由として、コンテンツの著作権保有者（または著作権管理者、以下、両者の概念を総称して著作権保有者と称する場合も有る）が未だ通信回線を利用したパソコンへの配信に関して不正コピーなどの心配から信用していないためである。このように、コンテンツ配信サービスは、ユーザからの要望あるいはビジネス的魅力があっても、不正流通の問題が足かせとなり、重要なコンテンツの配信には極めて消極的な状況にある。

#### 【0004】

一方、一部のマンションなどの販売事業者が、他社との差別化を目的に、著作権保有者から話題のコンテンツを購入し、自社マンション顧客内での通信回線を利用したサービス提供を行っている。しかし、このようなコンテンツの流通形態では、高額なコンテンツ購入料を必要とし、また、一般ユーザの加入が望めないという問題がある。

#### 【0005】

尚、本発明に係るシステムの先行技術例として、下記の特許文献1～5がある。

#### 【0006】

特許文献1には、記録制限情報付メモリーカードを用いたダウンロードシステムとして、メモリーカードのデータ領域の、相互認証成功後に読み書きできる保護領域に、記録制限情報鍵及びコンテンツ鍵を暗号化記録制限情報として記録させておき、不正なダウンロードの防止し、またダウンロードに対する課金を実現するための記録制限情報を安易に書き換えたり読み出したりできないようにしながら、記録制限情報に従ったコンテンツのダウンロードができる構成が記載されている。

#### 【0007】

特許文献2には、配信データが利用されるごとに使用機器から使用履歴情報を取得し、この使用履歴情報に基づいてデータ配信に伴う対価を関係エンティティに所望の割合で分配できるようにしたデータ配信システムの構成が記載されている。

#### 【0008】

特許文献 3 には、チャネル受信契約情報とチャネル送信契約情報とを統合して、指定されたコンテンツ情報に対応する利用可能契約情報リストを作成し、このリストに基づいてコンテンツ利用条件を決定し、この条件に基づいて受信コンテンツ情報の利用を制御する放送受信装置の構成が記載されている。

#### 【0 0 0 9】

特許文献 4 には、コンテンツをコンテンツ鍵によって暗号化して暗号化コンテンツを作成し、コンテンツの一部をサンプルデータとして抽出し、コンテンツ鍵を利用者情報によって暗号化した秘密鍵をサンプルデータに不可視情報として埋め込んだウォーターマーク入サンプルデータを作成し、これに暗号化コンテンツを合成した合成データを配信することで、著作権の侵害を防止し、かつ暗号化コンテンツを復号化するための許諾情報が破壊されたり、紛失したりすることを防止可能なデータ運用方法の構成が記載されている。

#### 【0 0 1 0】

特許文献 5 には、装置 I D、媒体 I D、データ暗号化鍵を用いて暗号化した許諾情報及び暗号化データを媒体に書き込み、データの読み出し時に、媒体から読み出した媒体 I D と許諾情報と自身の装置 I D からデータ復号鍵を復号し、この復号したデータ復号鍵を用いて媒体から読み出した暗号化データを復号するようにして、装置 I D を持った装置のみが復号化可能とし、媒体や復元プログラムが盗用されても暗号化データの復元を不可とし、媒体上の暗号化データの機密保持を図る機密保護システムの構成が記載されている。

#### 【0 0 1 1】

特許文献 6 には、著作権付コンテンツデータが再生可能に暗号化されて記録される媒体部と、著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、かつ記録処理を行う記録装置及び再生処理を行う再生装置の各々に対する認証機能を有する制御装置とを備えた情報記録媒体を用い、認証機能により認証され、かつ管理情報により記録／再生可能とされたときのみ、コンテンツデータを記録／再生でき、これによってコンテンツデータを記録しつつ、不正な利用から保護するシステムの構成が記載されている。

#### 【0 0 1 2】

## 【特許文献 1】

特開 2 0 0 1 - 3 4 4 2 1 6 号公報

## 【0 0 1 3】

## 【特許文献 2】

特開 2 0 0 1 - 3 0 6 9 5 4 号公報

## 【0 0 1 4】

## 【特許文献 3】

特開 2 0 0 0 - 3 4 9 7 2 5 号公報

## 【0 0 1 5】

## 【特許文献 4】

特開 2 0 0 0 - 3 3 9 2 2 7 号公報

## 【0 0 1 6】

## 【特許文献 5】

特開平 0 9 - 1 3 4 3 1 1 号公報

## 【0 0 1 7】

## 【特許文献 6】

特開 2 0 0 2 - 1 9 6 9 8 2 号公報

## 【0 0 1 8】

## 【発明が解決しようとする課題】

以上述べたように、コンテンツ配信サービスは、ユーザからの要望あるいはビジネス的魅力があっても、不正流通の問題が足かせとなって著作権保有者の信頼が得られず、重要なコンテンツの配信には極めて消極的な状況にある。

## 【0 0 1 9】

本発明は、以上のような実情を考慮してなされたもので、コンテンツの不正流通を阻止する著作権保護の仕組みを具備した形で、コンテンツの著作権保有者または著作権管理者から信頼を得ることにより、リーズナブル価格で通信回線を利用した有効なコンテンツの配信サービスを実現することのできるコンテンツ配信サービス提供装置と、そのサービスを受ける端末装置を提供することを目的とする。

**【 0 0 2 0 】****【課題を解決するための手段】**

上記の目的を達成するために、本発明に係るコンテンツ配信サービス提供装置は、以下のように構成される。

**【 0 0 2 1 】**

(1) 少なくとも媒体固有識別子及び媒体鍵情報の媒体情報が書き込まれた情報記憶媒体に、または前記情報記憶媒体がセットされた状態で前記情報記憶媒体とは別の情報記憶媒体にコンテンツを記録可能とするユーザ側の端末装置に対して、通信回線を介してコンテンツの配信サービスを行うコンテンツ配信サービス提供装置であって、前記配信サービスの加入申請を行うユーザの個人情報、サービス範囲、支払い方法を含むユーザ情報を事前登録し、ユーザ毎にサービス提供時の認証情報の配布、配信コンテンツ選択リストの配布及びコンテンツ選択要求受付、課金・決済を管理するユーザ管理制御装置と、前記配信サービスを行うコンテンツの著作権保有者または著作権管理者からコンテンツと共にコンテンツ鍵生成条件を取得し、前記コンテンツ鍵生成条件を基にコンテンツ鍵及びこのコンテンツ鍵による暗号化コンテンツを生成する暗号化コンテンツ制御装置と、前記暗号化コンテンツ制御装置で生成されるコンテンツ鍵を蓄積すると共に、前記情報記憶媒体の媒体情報の全部または一部を登録し、前記ユーザからのコンテンツ要求時に提示される媒体情報または媒体情報及び端末装置固有情報を用いて前記要求コンテンツに対応するコンテンツ鍵を暗号化し、この暗号化コンテンツ鍵を要求元ユーザの端末装置に発行する暗号化コンテンツ鍵制御装置と、前記暗号化コンテンツ制御装置で生成される暗号化コンテンツを蓄積し、前記ユーザからのコンテンツ要求時に該当する暗号化コンテンツを選択し、要求元ユーザの端末装置に配信するコンテンツ制御配信装置とを具備して構成される。

**【 0 0 2 2 】**

(2) (1) の構成において、前記ユーザ管理制御装置は、前記コンテンツ配信サービスの加入申請としてユーザ個人情報、サービス適用範囲、支払い方法を含むユーザ情報を提示したユーザの適否を判断するユーザ適否判断手段と、この判断手段で適正と判断された適正ユーザの前記ユーザ情報を管理するユーザ情報

管理手段と、前記ユーザに対してログイン用の認証情報を発行する認証情報発行手段と、前記認証情報に基づいてログインされたユーザ側の端末装置に対し、前記ユーザ情報管理手段で管理されるユーザ情報のサービス適用範囲から配信可能なコンテンツを選択しそのリストを提供するリスト提供手段と、前記ユーザ側の端末装置から前記リストに提示されるコンテンツの選択を受けて前記コンテンツ制御配信装置に該当するコンテンツの配信を指示する配信指示手段と、前記コンテンツの配信時に前記ユーザの課金・決済情報を管理する課金・決済管理手段とを備える。

#### 【0023】

(3) (2) の構成において、コンテンツ配信サービス提供装置は、さらに、前記コンテンツの配信を行う際に、前記ユーザ側の端末装置にコンテンツ取得用のアプリケーションを起動するための起動情報を配信する起動情報配信手段を備える。

#### 【0024】

(4) (1) の構成において、前記暗号化コンテンツ制御装置は、前記コンテンツを指定のデジタル符号化形式でエンコードする、あるいは指定のデジタル符号化形式に変換し、前記コンテンツ鍵生成条件に基づいてコンテンツ鍵を生成し、当該コンテンツ鍵により前記コンテンツを暗号化する暗号化コンテンツ生成手段と、前記暗号化コンテンツ生成部で暗号化された暗号化コンテンツを前記コンテンツ制御配信装置に発行する暗号化コンテンツ発行手段と、前記暗号化コンテンツ生成部で生成されたコンテンツ鍵を前記コンテンツ鍵制御装置に発行するコンテンツ鍵発行手段とを具備する。

#### 【0025】

(5) (1) の構成において、暗号化コンテンツ鍵制御装置は、前記暗号化コンテンツ制御装置で生成されるコンテンツ鍵を蓄積するコンテンツ鍵蓄積部と、前記情報記憶媒体の媒体情報の全部または一部を格納する媒体情報格納部と、前記ユーザからのコンテンツ要求時に、要求コンテンツに対応するコンテンツ鍵を前記コンテンツ鍵蓄積部から読み出し、ユーザから提示される媒体情報に基づいて前記コンテンツ鍵を暗号化する暗号化処理部と、前記暗号化処理部で生成され

た暗号化コンテンツ鍵を要求元に発行する暗号化コンテンツ鍵発行部とを具備する。

#### 【0026】

(6) (5) の構成において、前記暗号化コンテンツ鍵制御装置の暗号化処理部は、前記ユーザから前記媒体情報と共に提示される端末装置固有情報、コンテンツ識別情報、コンテンツ配信制御装置を識別するための情報、媒体連携コンテンツ取得装置を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ鍵個別情報の少なくともいずれかを取得し、これらの情報に基づいて前記コンテンツ鍵の暗号化を行う。

#### 【0027】

(7) (1) の構成において、コンテンツ制御配信装置は、前記暗号化コンテンツ制御装置で生成される暗号化コンテンツを蓄積する暗号化コンテンツ蓄積部と、前記ユーザからのコンテンツ要求時に前記暗号化コンテンツ蓄積部から該当する暗号化コンテンツを読み出し、前記暗号化コンテンツ鍵制御装置で生成される暗号化コンテンツ鍵に基づいて前記暗号化コンテンツを再暗号化する暗号化処理部と、前記暗号化処理部で生成された暗号化コンテンツを要求元に配信する配信処理部とを具備する。

#### 【0028】

(8) (1) の構成において、さらに、前記ユーザ側の端末装置との間で日時情報を同期させる日時情報同期手段を備える。

#### 【0029】

(9) (1) の構成において、さらに、前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置にそれぞれ暗号化コンテンツ鍵生成、暗号化コンテンツ配信に、任意のコンテンツ視聴条件、オプション情報を選択的に含める。

#### 【0030】

また、本発明に係るコンテンツ配信サービス端末装置は、以下のように構成される。

#### 【0031】

(10) (1) のコンテンツ配信サービス提供装置から前記コンテンツ配信サ



ービスを受けるコンテンツ配信サービス端末装置において、前記ユーザ管理制御装置との間で、前記認証情報に基づくログインを行い、前記配信コンテンツ選択リストに基づいてコンテンツ選択要求を行うユーザアクセス・コンテンツ選択装置と、前記コンテンツ選択要求時に、前記情報記憶媒体から前記媒体情報を取得して前記コンテンツ配信サービス提供装置に送り、前記コンテンツ配信サービス提供装置から暗号化コンテンツ鍵及び配信コンテンツを受け取って、共にまたは別々に前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体の書込可能領域に書き込む媒体連携コンテンツ取得装置と、前記情報記憶媒体から任意の暗号化コンテンツを読み出すと共に対応する暗号コンテンツ鍵を読み出し、前記暗号化コンテンツ鍵を前記媒体情報に基づいて復号し、復号されたコンテンツ鍵に基づいて暗号化コンテンツを復号するコンテンツ提示制御装置とを具備する。

#### 【0032】

(11) (10) の構成において、ユーザアクセス・コンテンツ選択装置は、前記ユーザ管理制御装置に予め提示される認証情報に基づいてログインし、要求される情報を提示するログイン手段と、前記アクセスにより前記ユーザ管理制御装置から提示される配信コンテンツ選択リストを取得して提示し、ユーザ指定のコンテンツ選択要求を前記ユーザ管理制御装置に通知するコンテンツ選択要求手段とを具備する。

#### 【0033】

(12) (10) の構成において、媒体連携コンテンツ取得装置は、前記コンテンツ選択要求時に、前記情報記憶媒体から前記媒体情報を取得し、この媒体情報または媒体情報及び端末装置固有情報を前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置に通知する情報通知手段と、前記暗号化コンテンツ鍵制御装置及び前記コンテンツ制御配信装置から暗号化コンテンツ鍵及び暗号化コンテンツを受け取り、共にまたは別々に前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体の書込可能領域に書き込む情報記憶手段とを具備する。

#### 【0034】

(13) (12) の構成において、媒体連携コンテンツ取得装置は、さらに、前記コンテンツ配信サービス提供装置から配信される起動情報によって起動し、前記コンテンツ配信サービス提供装置との間で相互認証を行い、認証確認後に前記情報通知手段及び情報記憶手段の処理実行を指示する起動手段を備える。

**【0035】**

(14) (10) の構成において、さらに、前記コンテンツ配信提供装置から提供される日時情報に基づいて処理を実行する日時情報管理手段を備える。

**【0036】**

(15) (10) の構成において、前記媒体連携コンテンツ取得装置は、前記コンテンツ配信サービス提供装置からコンテンツ視聴条件を受け取った場合、その視聴条件を前記媒体情報が書き込まれている情報記憶媒体または他の情報記憶媒体に書き込み、前記コンテンツ提示制御装置は、前記暗号化コンテンツ及び暗号化コンテンツ鍵の復号化の際に、前記コンテンツ視聴条件に基づいて処理を実行する。

**【0037】**

(16) (12) の構成において、媒体連携コンテンツ取得装置は、前記暗号化コンテンツ視聴条件が視聴期限を指定している場合、前記情報記憶媒体に書き込まれたコンテンツを日時情報により管理し、前記視聴期限の経過時に前記情報記憶媒体から前記コンテンツを使用不能にする。

**【0038】**

(17) (10) の構成において、前記コンテンツ提示制御装置は、前記媒体情報が書き込まれた情報記憶媒体とは別の情報記憶媒体に前記暗号化コンテンツ、暗号化コンテンツ鍵の少なくともいずれか一方が書き込まれている場合には、前記媒体情報が書き込まれた情報記憶媒体がセットされた状態でのみ前記暗号化コンテンツ及び暗号化コンテンツ鍵の読み出し、復号処理を実行する。

**【0039】**

**【発明の実施の形態】**

以下、図面を参照して本発明の実施の形態を詳細に説明する。

**【0040】**

図 1 は本発明に係るコンテンツ配信システムの構成を示す概念図である。このシステムは、コンテンツ配信サービスセンター側の装置（以下、センター側装置）100と、この装置100に通信回線300を通じてアクセスすることによりコンテンツ配信サービスを受けるユーザ側装置200とで構成される。

#### 【0041】

センター側装置100は、ユーザ管理制御装置110、暗号化コンテンツ生成部120、暗号化コンテンツ鍵制御装置130、コンテンツ制御配信装置140、オプション情報入力装置150、サーバ日時同期装置160を備える。ユーザ側装置200は、ユーザアクセス・コンテンツ選択装置210、媒体連携コンテンツ取得装置220、媒体情報（媒体鍵情報及び媒体固有識別子）を有する情報記憶媒体230、コンテンツ提示制御装置240、端末日時同期装置250、コンテンツ視聴装置260、媒体情報（媒体鍵情報及び媒体固有識別子）を有していない情報記憶媒体（以下、230の情報記憶媒体と区別するため、単に記憶媒体と記す）270を備える。

#### 【0042】

（センター側装置100）

ユーザ管理制御装置110は、まず、ユーザが通信回線300を利用してコンテンツの選択を行うにあたり、ユーザから提供されるサービス加入申請に必要な各種要件、支払い方法の情報を受け取って、申請ユーザがサービスを受けられる適合者か否かの判定を行う。

#### 【0043】

サービス加入申請の手続き方法としては、電話によるオペレータへの口頭連絡、郵送による書面提出、ユーザアクセス・コンテンツ選択装置210によるデータ通信といった方法がある。サービス加入申請に必要な要件の情報としては、例えば、氏名、生年月日、住所、性別、電話番号、加入サービスのタイプ（例えば、映画コンテンツのみの視聴、スポーツコンテンツのみ視聴、全てのコンテンツを視聴等）がある。支払い方法としてはプリペイドカード方式、クレジットカード方式等があり、その情報としては、例えばプリペイドカード番号、クレジットカード番号、カードの有効期限等がある。

**【0044】**

上記の要件判定に際し、支払い方法がクレジットカードである場合には、決済代行会社に必要な情報を発信し、支払い可能か否かの確認を行う。支払い可能である場合、決済代行会社から決済用識別子を受け取り、登録する。このとき、クレジットカード情報漏洩の危険性を回避するため、登録情報からクレジットカード番号及びクレジットカードの有効期限等の情報を消去しておく。

**【0045】**

判定の結果、申請ユーザがサービスを受けられない不適合者であると判定した場合、申請ユーザにサービス加入不可の旨を口頭、書面、ユーザアクセス・コンテンツ選択装置 210 のいずれかを通じて通知する。申請ユーザがサービスを受けられる適合者であると判定した場合、サービス許可ユーザとして登録し、ユーザから提供された情報を蓄積する。そして、申請ユーザに口頭、書面、ICカード等の記憶媒体、ユーザアクセス・コンテンツ選択装置 210 のいずれかを通じて、ログインする際に必要となる認証条件（ユーザID、パスワード等）を発行する。

**【0046】**

ここで、記憶媒体あるいはユーザアクセス・コンテンツ選択装置 210 を通じて認証条件を発行する場合には、ユーザを特定する識別子（ユーザID）あるいはユーザ側で使用する装置を特定するための識別子（装置ID）を暗号化して発行するようにしてもよい。

**【0047】**

ユーザ管理制御装置 110 は、ユーザアクセス・コンテンツ選択装置 210 によって上記の認証条件に基づいてログインしたユーザに対し、該当するユーザ情報を読み出し、登録されているサービスタイプからどのようなサービス（範囲）を受けられるユーザであるかを判定し、ログインユーザのユーザアクセス・コンテンツ選択装置 210 に認証情報を発行する。この認証情報に基づいてユーザアクセス・コンテンツ選択装置 210 からコンテンツリスト表示要求があった場合には、要求ユーザに見合ったコンテンツリスト及びフォーマットを選択し、選択したコンテンツリストをユーザアクセス・コンテンツ選択装置 210 が表示可能な

フォーマット形式等に編集し、ユーザアクセス・コンテンツ選択装置 2 1 0 に発行する。

#### 【0 0 4 8】

また、ユーザ管理制御装置 1 1 0 は、ユーザアクセス・コンテンツ選択装置 2 1 0 からのコンテンツ選択を受け付け、コンテンツ配信前または配信後に、課金に関する要件を満たせるかの確認を、決済代行会社に対して先に決済代行会社から受け取った決済用識別子を基に行う（この確認処理を与信という）。選択したコンテンツが購入不可能な場合、その旨を与信情報としてユーザアクセス・コンテンツ選択装置 2 1 0 に通知する。選択したコンテンツが購入可能である場合、その旨を与信情報としてユーザアクセス・コンテンツ選択装置 2 1 0 に通知し、ユーザが本当に購入するか否かを再度問い合わせる。ユーザが最終的に購入確認を行った場合、課金・決済用の情報として蓄積すると共に、何時どんなコンテンツを選択・購入したか、及びコンテンツ視聴条件の情報をユーザ情報として蓄積する。

#### 【0 0 4 9】

暗号化コンテンツ制御装置 1 2 0 は、コンテンツの著作権保有者、または著作権管理者から、コンテンツと、このコンテンツの暗号化／復号化に使用するコンテンツ鍵を生成するための条件を取得し、この条件に基づいてコンテンツ鍵を生成し、このコンテンツ鍵に基づいてコンテンツを暗号化して、暗号化コンテンツ及びコンテンツ鍵の発行処理を行う。尚、コンテンツには電子透かしを埋め込んでおくと、不正コピー発覚時のコンテンツ提供元がわかり、効果的である。

#### 【0 0 5 0】

暗号化コンテンツ鍵制御装置 1 3 0 は、暗号化コンテンツ制御装置 1 2 0 にて生成されたコンテンツ鍵を暗号化コンテンツに対応付けて蓄積する。そして、コンテンツ配信制御装置 1 4 0 等からのコンテンツ識別情報と、通信回線 3 0 0 を介して媒体連携コンテンツ取得装置 2 2 0 から取得した情報記憶媒体 2 3 0 の媒体情報（情報記憶媒体 2 3 0 の読込専用領域に書き込まれている媒体鍵情報及び媒体固有識別子）とを受け付け、コンテンツ識別情報をもとに暗号化コンテンツに対応するコンテンツ鍵を選択し、そのコンテンツ鍵を予め登録されている装置

固有鍵情報及び情報記憶媒体 2 3 0 の媒体情報をもとに暗号化して暗号化コンテンツ鍵を生成し、コンテンツ配信制御装置 1 4 0 等の要求元に発行する。また、オプション情報が与えられた場合には、このオプション情報を含んだ形で暗号化コンテンツ鍵を生成して要求元に発行する。

#### 【0 0 5 1】

オプション情報としては、コンテンツ配信制御装置 1 4 0 を識別するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などがある。これらのオプション情報は、コンテンツ配信制御装置 1 4 0、媒体連携コンテンツ取得装置 2 2 0 などの装置から受け取る、あるいはオプション情報入力装置 1 5 0 から直接取得する。

#### 【0 0 5 2】

ここで、上記の情報記憶媒体 2 4 0 の媒体情報、コンテンツ配信制御装置 1 4 0 の識別情報、媒体連携コンテンツ取得装置 2 2 0 の識別情報、ユーザ識別情報、コンテンツ視聴条件情報、コンテンツの制御付随情報などは、コンテンツ配信制御装置 1 4 0 を介して受け渡される以外に、媒体連携コンテンツ取得装置 2 2 0 等のその他の装置から取得する、あるいは入力装置の入力操作によって直接取得するようにしてもよい。

#### 【0 0 5 3】

尚、コンテンツ鍵自体は、センター内のセキュリティあるいは外部からのハッキングを考慮して、暗号化コンテンツ制御装置 1 2 0 または暗号化コンテンツ鍵制御装置 1 3 0 で暗号化して蓄積しておくことが望ましい。この場合、暗号化コンテンツ鍵制御装置 1 3 0 では、コンテンツ鍵を暗号化した状態で蓄積しておき、コンテンツ配信制御装置 1 4 0 などからの暗号化コンテンツ鍵発行要求を受けた時点で、該当する暗号化されたコンテンツ鍵を読み出して復号し、コンテンツ識別情報、情報記録媒体 2 3 0 の媒体情報、コンテンツ配信制御装置 1 4 0 を識

判するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ鍵個別情報など、これら情報の単数または複数の組み合わせと装置固有鍵情報の情報とを基に再びコンテンツ鍵を暗号化して発行する。

#### 【 0 0 5 4 】

上記コンテンツ鍵個別情報は、コンテンツの著作権保有者から受けるコンテンツ鍵生成条件の中に含まれる情報、あるいは暗号コンテンツの生成、コンテンツ鍵の発行といった処理過程で暗号化を行う際に独自に生成され、復号に利用する情報を意味する。

#### 【 0 0 5 5 】

コンテンツ制御配信装置 1 4 0 は、暗号化コンテンツ制御装置 1 2 0 にて生成された暗号化コンテンツを複数蓄積し、ユーザ管理制御装置 1 1 0 からユーザが選択したコンテンツ情報とユーザ情報（コンテンツ視聴条件等）を受け付け、ユーザ側装置 2 0 0 及びその装置に搭載あるいは接続された情報記憶媒体 2 3 0 と連携し、暗号化コンテンツ及び暗号化コンテンツ鍵等を配信する。

#### 【 0 0 5 6 】

ここで、コンテンツ制御配信装置 1 4 0 は、ユーザ側装置 2 0 0 及び情報記憶媒体 2 3 0 と連携するにあたって、ユーザ側装置 2 0 0 内の連携アプリケーションを起動させる必要があるため、連携アプリケーション起動のための起動情報をユーザ側装置 2 0 0 に対して発行し、起動情報による相互認証を実施する。すなわち、起動情報の相互認証が完了したことを条件に、通信回線 3 0 0 を介した媒体情報の発行及び配信コンテンツの情報記憶媒体 2 3 0 への書き込み等を可能にする。これにより、例えば過去に不正アクセスしたユーザ等の特定のユーザ側装置 2 0 0 の通信機能を動作不能とする動作制限が可能となり、セキュリティ向上を図ることができる。

#### 【 0 0 5 7 】

上記起動情報は、ユーザ側装置 2 0 0 の連携アプリケーションが情報漏洩対策などの理由から暗号化されている場合には、ユーザ管理制御装置 1 1 0 でログイン時に生成された認証情報、ユーザ管理制御装置 1 1 0 に蓄積されているユーザ

情報、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体 2 7 0、ユーザアクセス・コンテンツ選択装置 2 1 0 に保管されたユーザを特定する識別子あるいは機器を特定するための識別子などをもとに起動情報を生成し、必要に応じて暗号化し、発行する。

#### 【0 0 5 8】

また、コンテンツ配信制御装置 1 4 0 は、コンテンツを配信するにあたって、ユーザ側装置 2 0 0 あるいは情報記録媒体 2 3 0 との連携を実現するためのインターフェースに対し、レスポンス要求（ping コマンド等のレスポンスを利用し、通信回線の状況把握をしてもよい）を行い、その応答を解析することにより通信回線の負荷を把握する。これを繰り返し、ユーザ側装置 2 0 0 に対して配信可能な通信回線で一番妥当な（負荷が少ない等）通信回線を選択し、選択したコンテンツの容量と解析された通信回線負荷等の情報からコンテンツの配信が終了するまでの想定時間を算出して、この情報を発行可能とする。また、最終的に何時までにコンテンツ配信を終了させたいか等の予約配信の指定を発行可能とし、候補を複数選出し、現在の時間に近い順あるいは優先度指定によりコンテンツ配信を行う。

#### 【0 0 5 9】

また、コンテンツ配信制御装置 1 4 0 は、ユーザ管理制御装置 1 1 0 などに蓄積されているコンテンツ視聴条件（視聴期間が制限されたコンテンツであることを示す情報、視聴可能日時（期限）情報、情報記憶媒体への書込制限情報、コンテンツ保護情報、年齢制限情報、バリアフリー対応情報（手話種別・識別情報等）等）を受け付け、必要に応じて暗号化を行い、発行する。

#### 【0 0 6 0】

ここで、暗号化コンテンツ視聴条件あるいはコンテンツ視聴条件中に、必要に応じてコンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）、電子透かし制御情報（例えば表示のオン・オフフラグ）等）などを含めるようにしてもよい。

#### 【0 0 6 1】



また、コンテンツ配信制御装置 1 4 0 は、ユーザ側装置 2 0 0 を識別するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報、外部リンク情報、ガイダンス情報などのオプション情報を、必要に応じて暗号化コンテンツ及び暗号化コンテンツ鍵と紐付けし、必要に応じて暗号化を行い、暗号化オプション情報として発行する。

#### 【 0 0 6 2 】

サーバ日時同期装置 1 6 0 は、公知の日時発行装置等から通信回線を利用して正確な日時を取得し、要求に応じて保持している日時を要求元に発行する。

#### 【 0 0 6 3 】

(ユーザ側装置 2 0 0)

ユーザアクセス・コンテンツ選択装置 2 1 0 は、ユーザが通信回線 3 0 0 を利用してセンター側装置 1 0 0 へアクセスしてコンテンツを選択し、コンテンツの購入確認に至る、通信回線を利用した著作権保護コンテンツ配信サービスを受けるための一連の手続処理を行うマンマシン・インターフェース、通信インターフェースを有する情報処理装置であり、例えば、パソコン、セットトップボックス、A V 機器、家電機器等、通信回線を介してサービスとの連携を可能にする装置である。

#### 【 0 0 6 4 】

具体的には、ユーザ管理制御装置 1 1 0 との間で、サービス加入申請情報の送付、認証条件の取得、認証条件に基づくログイン、コンテンツリストの取得及び表示・閲覧、コンテンツリストからのコンテンツ選択情報の送付等の処理を行う。ユーザがコンテンツリスト表示内容を閲覧してコンテンツ選択を行う際には、コンテンツ視聴条件（例えば、ある一定期間のみコンテンツ視聴が可能なタイプか、期間制限なしのコンテンツ視聴が可能なタイプか等）も同時に選択する。

#### 【 0 0 6 5 】

媒体連携コンテンツ取得装置 2 2 0 は、情報記憶媒体 2 3 0 とセンター側のコンテンツ配信制御装置 1 4 0 との連携アプリケーションを備え、ユーザアクセス・コンテンツ選択装置 2 1 0、コンテンツ配信制御装置 1 4 0、ユーザ自身のい

ずれかからの起動要求に従い、コンテンツ配信制御装置 1 4 0 から暗号化コンテンツ及び暗号化コンテンツ鍵等を取得する。

#### 【0 0 6 6】

その手法としては、情報記憶媒体 2 3 0 の媒体情報をコンテンツ配信制御装置 1 4 0 に送付し、日時情報を取得すると共に、コンテンツ配信制御装置 1 4 0 と連携して、当該コンテンツ配信制御装置 1 4 0 から通信回線 3 0 0 を介して送られてくる暗号化コンテンツと暗号化コンテンツ鍵を情報記憶媒体 2 3 0 の書込可能領域に書き込む。そして、暗号化コンテンツ及び暗号化コンテンツ鍵等が全て正常に情報記憶媒体 2 3 0 の書込可能領域に書き込まれたかチェックし、正常に書き込まれた場合には、その結果を日時情報と併せてコンテンツ配信制御装置 1 4 0 に通知する。コンテンツ配信制御装置 1 4 0 では、この通知情報を基に当該ユーザの最終的な課金・決済情報を発行し、この情報をユーザ管理制御装置 1 1 0 に通知する。

#### 【0 0 6 7】

但し、上記の方法では、ユーザ側で正常書き込みを通知する前にネットワークを切断した場合、課金されないケースが想定される。このため、コンテンツ配信制御装置 1 4 0 において、暗号化コンテンツの送付後、先に課金処理を行い、あるいは課金処理を行った後に暗号化コンテンツを送付する。ここで、書き込み異常の通知（再発行要求）があった場合には再送付処理を行い、正常書き込み通知を受けた場合には、暗号化コンテンツ鍵を送付し、この鍵の正常書き込み通知を受けた場合に一連の処理を終了する流れとする方法が有効である。

#### 【0 0 6 8】

ここで、情報記憶媒体 2 3 0 との連携、あるいはコンテンツ配信制御装置 1 4 0 との連携を行う連携アプリケーションの実行に関しては、情報漏洩対策などの理由からアプリケーション自体が暗号化され、起動にあたっては起動情報などが必要となる場合がある。この場合、ユーザ管理制御装置 1 1 0 にてログイン時に生成された認証情報、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体（ＩＣカード等） 2 7 0、ユーザアクセス・コンテンツ選択装置 2 1 0 に保管されたユーザを特定する識別子、ユーザ側装置 2 0 0 を特定するための識別子などの

情報を、コンテンツ配信制御装置 1 4 0 に通知し、コンテンツ配信制御装置 1 4 0 から起動情報を取得するか、通信回線 3 0 0 を利用していないスタンドアロン状態などにおいては、先に取得した情報を用いて、独自に起動情報を生成し、起動させる。起動後、前述の起動情報による相互認証を行う。

#### 【0 0 6 9】

また、コンテンツ配信制御装置 1 4 0 から暗号化オプション情報を受け付けた際には、前述の起動情報を利用して暗号化オプション情報を復号してオプション情報を取得する。このとき、オプション情報に含まれるコンテンツ配信制御装置 1 4 0 を識別するための情報、本装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報などを解析し、この情報に基づくチェックを行い、これに準拠した形で動作制限等の制御、記憶媒体（I C カード等）2 7 0 の記憶情報の更新、保管を行い、これらの情報を必要に応じて情報記憶媒体 2 3 0 の書込可能領域に書き込む。

#### 【0 0 7 0】

また、情報記憶媒体 2 3 0 への書き込み処理を行う際、コンテンツ配信制御装置 1 4 0 から通知されるコンテンツ視聴条件等の情報を受け付ける。この情報のコンテンツ視聴条件が期間制限されたコンテンツ視聴タイプ、つまりコンテンツを一定期間のみ視聴可能とする条件付き視聴のタイプである場合、コンテンツ視聴タイプを示す情報と日時情報を暗号化し、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体（I C カード等）2 7 0 に保管するか、あるいはこれらの情報を情報記憶媒体 2 3 0 の書込可能領域に書き込む。

#### 【0 0 7 1】

情報記憶媒体 2 3 0 は、例えば D V D - R A M ディスク等であり、予め読込専用領域に媒体鍵情報、媒体固有識別子が書き込まれている。媒体鍵情報、媒体固有識別子は、いずれも要求に応じて読み出し出力することが可能である。また、書込可能領域には、媒体連携コンテンツ取得装置 2 2 0 を通じて与えられる暗号化コンテンツ、暗号化コンテンツ鍵、暗号化視聴条件、オプション情報などを書込可能とする。

**【0072】**

コンテンツ提示制御装置 2 4 0 は、予めユーザ側装置 2 0 0 が保有する装置固有鍵情報と情報記憶媒体 2 3 0 の読込専用領域にある媒体情報に基づいて書込可能領域に書き込まれている暗号化コンテンツ鍵を復号してコンテンツ鍵を生成し、このコンテンツ鍵をもとに暗号化コンテンツを復号し、提示可能とする。ここで、媒体連携コンテンツ取得装置 2 2 0 にて取得し、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体（ＩＣカード等） 2 7 0 あるいは情報記憶媒体 2 3 0 の書込可能領域に保管されているオプション情報がある場合、これを読み出し、この情報に基づく提示処理を行う。

**【0073】**

また、媒体連携コンテンツ取得装置 2 2 0 にて取得し、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体（ＩＣカード等） 2 7 0 に保管されているか、情報記憶媒体 2 3 0 の書込可能領域に保管されている暗号化された視聴条件がある場合、これを読み出し、併せて端末日時同期装置 2 5 0 から情報を取得し、既に蓄積されているコンテンツが期間を超過しているかのチェックを行い、超過している場合はユーザに対してこの旨を通知し、コンテンツが使用不能となるように処理する。

**【0074】**

端末日時同期装置 2 5 0 は、ユーザ側装置 2 0 0 において、通信回線 3 0 0 を介してサーバ日時同期装置 1 6 0 から日時を取得し、媒体連携コンテンツ取得装置 2 2 0 などからの要求を受け付け、日時を発行する。但し、この装置 2 5 0 は、ユーザ側でセット可能なタイマーとは異なり、外部から設定不可能な日時保持方式を有する。あるいは、ユーザ側装置 2 0 0 でセット可能なタイマーを用いる場合には、タイマーの日時を強制的に外部からサーバ側に同期して最新日時に更新されるようにしてもよい。尚、この端末日時同期装置 2 5 0 は、必ずしもユーザ側装置 2 0 0 に含める必要はなく、サーバ日時同期装置 1 6 0 から直接情報を取得するようにしてもよい。

**【0075】**

コンテンツ視聴装置 2 6 0 は、コンテンツ提示制御装置 2 4 0 からのコンテン

ツ提示情報を受け付け、ユーザがコンテンツ視聴を可能にするディスプレイ、TV等の装置である。

#### 【0076】

以上のように構成されたコンテンツ配信システムによれば、通信回線を利用して簡単なアクセス及びコンテンツ選択をすることにより、著作権が保護された形でコンテンツが所定の情報記憶媒体230上に書き込まれ、ユーザの要求によるコンテンツの視聴（再生・閲覧）が可能になり、様々な形態の料金設定、料金の徴収、様々な形態のコンテンツの取得、タイムリーなサービス等が効率良く行えるようになり、ユーザが店頭に行ってコンテンツを購入あるいはレンタルするといった手間を省くことが可能になる。

#### 【0077】

ここで、媒体連携コンテンツ取得装置220とコンテンツ配信制御装置間140は通信回線300を使用する。その他装置間は、通信回線300の他、直接接続された線、回路、記憶媒体等の利用を含むその他情報伝達手段を用いてもよい。

#### 【0078】

また、媒体連携コンテンツ取得装置220は、ユーザアクセス・コンテンツ選択装置210内に搭載あるいは、接続されている場合と、単独で存在する場合のどちらでもよいものとする。

#### 【0079】

また、情報記憶媒体230とは、DVD-RAMディスクなど読取専用領域と書込可能領域を併せ持ち、読込専用領域には各種ユーザ機器に対応した媒体鍵情報と媒体毎に保有する媒体固有識別子が存在するものであり、ディスク状の媒体に限らず、テープ状の媒体あるいは、半導体情報媒体等（メモリ、ICカード等）を用いてもよい。

#### 【0080】

また、記憶媒体270とは、DVD-RAMディスクなど読取専用領域と書込可能領域を併せ持つ情報記憶媒体に限らず、ディスク上の媒体、テープ上の媒体、半導体情報媒体等（メモリ、ICカード等）情報を記憶することの可能な媒体

を示す。

#### 【0081】

尚、上記実施形態において、暗号化コンテンツ鍵と暗号化コンテンツが保管される場所は、読込専用領域に媒体情報が存在する情報記憶媒体に限らず、別の記憶媒体でもよい。例えば、暗号化コンテンツはハードディスクに保管し、暗号化コンテンツ鍵は I C カード、D V D 媒体等の情報記憶媒体に記憶するようにしてもよい。また、暗号化コンテンツと暗号化コンテンツ鍵共にハードディスクに保管し、I C カード、D V D 媒体等の情報記憶媒体がユーザ側装置で読み出し可能な状態となっていれば、ダウンロードも視聴も可能とするような形態でもよい。

#### 【0082】

また、上記実施形態において、情報記憶媒体 2 3 0 として D V D 媒体を利用する場合、媒体連携コンテンツ取得装置 2 2 0 の連携アプリケーションは、D V D 媒体の読込専用領域にある M K B (Media Key Block: 媒体鍵情報) ハッシュ値 (M K B 識別情報として M K B と同様に D V D の読込専用領域に存在する) 及び媒体識別子 (Media ID) を読み取り、コンテンツ配信アプリケーションを介して暗号化コンテンツ鍵生成アプリケーションに送るようにするようにしてもよい。

#### 【0083】

これに対し、暗号化コンテンツ鍵制御装置 1 3 0 では、全部または一部のパターンの M K B についてライセンスを受けて蓄積しておき、ユーザ側装置 2 0 0 から送られてきた M K B 識別情報 (ハッシュ値) をもとに対象の M K B を選択し、この M K B とサーバ側の装置固有鍵情報とユーザ側装置 2 0 0 から送られてきた媒体識別子をもとに暗号化コンテンツ鍵を生成するようにしてもよい。

#### 【0084】

ここで、M K B を全パターン保有する場合は、ユーザ側から M K B の送付を受ける必要がなくなる。但し、ユーザ側装置 2 0 0 から送られてきた M K B 識別情報に対応する M K B が存在しない場合にはエラーステータス等を返すことになり、ユーザ側の困惑を招くおそれがある。また、ライセンス料が高くなる可能性もある。

#### 【0085】

これに対し、MKBを複数パターンのみ保有し、ユーザ側装置200から送られてくるハッシュ値に対応するMKBが存在しない場合には、MKB自体をユーザのDVD媒体から受け取るようにしてもよい。この方法は、ライセンス料が比較的安くすむ可能性があるが、MKBが正当なものかどうか判断が困難になることを考慮する必要がある。

#### 【0086】

さらに、本発明に係るシステムでは、ユーザのサービス範囲として、移動体向け（PDA等）、固定受信装置向け、あるいは視聴形態に応じて符号化形式を選択的に切り替えて配信し、それぞれの形式に応じた課金を行うようにしてもよい。

#### 【0087】

また、コンテンツ視聴条件として、条件そのものの情報をユーザ側装置200に送るのではなく、条件が提示されるサーバのアドレス（提示場所）を示すようにしてもよい。

#### 【0088】

（実施例）

以下、実施例について図2を参照して説明する。

#### 【0089】

（センター側装置100）

ユーザ管理制御装置110は、ユーザ管理部（ユーザ情報蓄積部F1を含む）111と、決済代行処理部112と、ユーザ認証部113と、コンテンツリスト表示・選択部（コンテンツリストフォーマット蓄積部F2を含む）114と、課金・決済部（課金・決済情報蓄積部F3を含む）115とから構成される。個々のブロック111～115の処理内容を図3及び図4に示す。

#### 【0090】

ユーザ管理部111では、ユーザから加入申請時に提示される各種要件（例えば、氏名、生年月日、住所、性別、電話番号、加入サービスのタイプ（例えば、映画コンテンツのみの視聴、スポーツコンテンツのみ視聴、全てのコンテンツを視聴等）、支払い方法（例えば、クレジットカード番号、クレジットカードの有

効期限等)の情報を入力し、ユーザがサービス提供に適するか否かを判定する。

#### 【0091】

具体的には、図3に示すように、サービス加入申請の種別を判断し(S111-1)、ユーザアクセス・コンテンツ選択装置210からの通知による場合には、その通知によって提示されるサービス加入申請情報の入力受付処理を行い(S111-2)、電話による口頭あるいは郵送による書面提出の場合には、オペレータによりユーザが提示したサービス加入申請情報の入力受付処理を行う(S111-3)。このとき、ユーザ情報蓄積部F1を参照して申請ユーザの過去の履歴に関する情報を取得し(S111-4)、ユーザ加入申請情報の入力内容をチェックする(S111-5)。

#### 【0092】

次に、ユーザ管理部110は、支払い方法がクレジットカードか否かを判断し(S111-6)、クレジットカードである場合には、決済代行処理部112に対して、ユーザの氏名、生年月日、住所、性別、電話番号、クレジットカード番号、クレジットカードの有効期限等の情報を発行する(S111-7)。

#### 【0093】

ここで、決済代行処理部112は、これらの情報を受け付け(S112-1)、受付内容をチェックした後(S112-2)、最良な決済代行会社を選択し(S112-3)、その決済代行会社に必要な情報の生成を行い(S112-4)、予め取り決めされた情報連携形態を検出し(S112-5)、その形態で決済代行会社へ情報を発信し(S112-6)、決済代行会社からの回答を受け付けて(S112-7)、申請ユーザが支払い可能か否かの確認を行う(S112-8)。支払いが可能である場合、決済代行会社から発行させる決済用識別子を受け取ってユーザ管理部111に発行し(S112-9)、支払いが不可能である場合、決済代行会社からNGステータスを受け取ってユーザ管理部111に発行する(S112-10)。

#### 【0094】

ユーザ管理部111は、決済代行処理部112からの決済用識別子またはNGステータスの回答を受け付ける(S111-8)。ここで、支払い可能であるこ



とを示す決済用識別子であるか否かを判断し（S 1 1 1 - 9）、決済用識別子の場合には、クレジットカード情報漏洩の危険性を回避するため、クレジットカード番号及びクレジットカードの有効期限等の情報を消去する（S 1 1 1 - 1 0）。支払い不可能であることを示す N G ステータスの場合には、サービス加入申請の種別を判断して（S 1 1 1 - 1 1）、サービス加入不可の旨をユーザアクセス・コンテンツ選択装置 2 1 0 を通じてユーザに通知するか（S 1 1 1 - 1 2）、あるいはオペレータが使用している端末等に通知し（S 1 1 1 - 1 3）、オペレータ等がユーザに対して電話にて口頭で通知するか、書面の郵送などで通知する。

#### 【0 0 9 5】

一方、ステップ S 1 1 1 - 6 で支払い方法がクレジットカードではないと判断された場合には、支払い方法の内容をチェックしてユーザ適否の審査を行う（S 1 1 1 - 1 4）。この審査で申請ユーザのサービス加入が可能か否かを判断し（S 1 1 1 - 1 5）、サービスを受けられると判定した場合には、最終的にサービスを受けるか否かの最終確認をユーザに通知し（S 1 1 1 - 1 6）、サービス加入の要求の有無を判断する（S 1 1 1 - 1 7）。

#### 【0 0 9 6】

サービス加入を受けるとの確認がとれた場合、ログインする際に必要となる認証条件（ユーザ I D、パスワード等）を生成し（S 1 1 1 - 1 8）、サービス加入申請の種別を判断して（S 1 1 1 - 1 9）、ユーザアクセス・コンテンツ選択装置 2 1 0 を通じて認証条件をユーザに発行し（S 1 1 1 - 2 0）、あるいはオペレータ等を通じて認証条件をユーザに発行し（S 1 1 1 - 2 1）、各種要件、決済用識別子、認証条件等の情報をユーザ情報蓄積部 F 1 に保管する（S 1 1 1 - 2 2）。一方、ステップ S 1 1 1 - 1 7 でサービス加入を受けるとの確認がとれなかった場合には、申請により受け付けた情報の内容を全て消去する（S 1 1 1 - 2 3）。

#### 【0 0 9 7】

尚、ユーザ管理部 1 1 1 は、ユーザに発行した認証条件を口頭、書面により直接通知するか、記憶媒体（I C カード等）、ユーザアクセス・コンテンツ選択装

置 2 1 0 を介して通知する。但し、記憶媒体あるいはユーザアクセス・コンテンツ選択装置 2 1 0 で認証条件を通知する場合には、情報の漏洩を考慮して、暗号化された形でユーザを特定する識別子あるいは機器を特定するための識別子を発行することが望ましい。

#### 【0 0 9 8】

ユーザがユーザ管理部 3 1 0 で発行された認証条件を取得し、この認証条件に基づいて、ユーザアクセス・コンテンツ選択装置 2 1 0 を利用し、通信回線 3 0 0 を介してログインした場合、ユーザ認証部 1 1 3、コンテンツリスト表示選択部 1 1 4 及び課金・決済部 1 1 5 は図 4 に示す処理を実行する。

#### 【0 0 9 9】

まず、ユーザ認証部 1 1 3 は、ログイン要求を受け付け（S 1 1 3 - 1）、認証情報を取得し（S 1 1 3 - 2）、ユーザ情報蓄積部 F 1 に蓄積されている情報を取得し（S 1 1 3 - 3）、ログイン可能かの判定を行う（S 1 1 3 - 4）。ログイン不可である場合、この旨を通知し（S 3 3 0 - 5）、可能である場合、ユーザ情報蓄積部 F 1 に蓄積されているサービスタイプから、どのようなサービス（範囲）を受けられるユーザであるかの情報を取得し（S 1 1 3 - 6）、取得した情報に基づく認証情報を生成して（S 1 1 3 - 7）、ユーザが利用しているユーザアクセス・コンテンツ選択装置 2 1 0 に認証情報を発行する（S 1 1 3 - 8）。

#### 【0 1 0 0】

コンテンツリスト表示・選択部 1 1 4 は、ユーザ認証部 1 1 3 にてユーザアクセス・コンテンツ選択装置 2 1 0 に発行された認証情報、あるいは、ユーザからのログインを受け付けたユーザ認証部 1 1 3 からの継承情報（ユーザ情報等）に基づいてユーザからのコンテンツリスト表示要求を受け付け（S 1 1 4 - 1）、要求したユーザに見合ったコンテンツリストフォーマットを判定して（S 1 1 4 - 2）、コンテンツリストフォーマット蓄積部 F 2 から選択し（S 1 1 4 - 3）、ユーザアクセス・コンテンツ選択装置 2 1 0 が表示可能な形式等に変換し（S 1 1 4 - 5）、ユーザアクセス・コンテンツ選択装置 2 1 0 に発行する（S 1 1 4 - 6）。

**【0101】**

このとき、ユーザはコンテンツリスト表示・選択部114にて発行されたコンテンツリストをユーザアクセス・コンテンツ選択装置210で表示・閲覧し、この表示に基づいて取得したいコンテンツの選択を行う。この際、コンテンツ視聴条件（例えば、ある一定期間のみコンテンツ視聴が可能なタイプか、期間制限なしのコンテンツ視聴が可能なタイプか等）の選択もコンテンツリスト表示に従い行う。

**【0102】**

課金・決済部115は、ユーザアクセス・コンテンツ選択装置210からのコンテンツ選択を受け付け（S115-1）、併せてコンテンツリスト表示・選択部210から継承情報を取得し（S115-2）、課金に関する要件を満たせるかの確認情報をユーザ管理部111に対して発行する（S115-3）。ユーザ管理部111はこれを受け付け、必要な情報をユーザ情報蓄積部F1から取得し、決済代行処理部112と連携して判定して、その判定結果を確認情報として課金・決済部115に通知する。

**【0103】**

課金・決済部115は、ユーザ管理部111から確認情報を受け取ると（S115-4）、その確認情報の判定結果から選択したコンテンツが購入可能かどうか判断する（S115-5）。選択したコンテンツが購入不可能な場合、その旨を与信情報としてユーザアクセス・コンテンツ選択装置210に通知し（S350-6）、選択したコンテンツが購入可能である場合、その旨を与信情報としてユーザアクセス・コンテンツ選択装置210に通知し（S350-7）、ユーザが本当に購入するか否かの確認を再度問い合わせする（S115-8）。

**【0104】**

上記確認の結果、ユーザが最終的に購入しない場合にはコンテンツ再選択を行う旨を通知し（S115-9）、購入確認を行った場合には、課金・決済用の情報として課金・決済情報蓄積部F3に蓄積する（S115-10）と共に、ユーザが何時どんなコンテンツを選択・購入したか、及び、コンテンツ視聴条件の情報をユーザ情報蓄積部F1に蓄積し（S115-11）、ユーザが選択したコン

テンツ情報とユーザ情報（コンテンツ視聴条件等）を発行する（S 1 1 5 - 1 2）。

#### 【0 1 0 5】

暗号化コンテンツ制御装置 1 2 0 は、暗号化コンテンツ生成部 1 2 1 と、暗号化コンテンツ発行部 1 2 2 と、コンテンツ鍵発行部 1 2 3 とから構成される。個々のブロック 1 2 1 ～ 1 2 3 の処理内容を図 5 に示す。

#### 【0 1 0 6】

暗号化コンテンツ生成部 1 2 1 は、コンテンツの著作権保有者から提供されたコンテンツ、及び、暗号化されたコンテンツを復号化する際のコンテンツ鍵生成条件を指定あるいは入力する（S 1 2 1 - 1、S 1 2 1 - 2）。ここで、コンテンツがデジタル符号化（A V I、M P E G - 1、M P E G - 2、M P E G - 4 等）された形式でない場合には、併せてエンコーディングする指定を行い（S 1 2 1 - 3、S 1 2 1 - 4）、デジタル符号化（A V I、M P E G - 1、M P E G - 2、M P E G - 4 等）された形式である場合でも、符号化形式の形式変換指定を行うことにより、復号した際のコンテンツ符号化形式の指定を可能にする（S 1 2 1 - 5、S 1 2 1 - 6）。コンテンツ鍵生成条件に関しては、手入力などの直接入力に対応してもよいが、テキストファイル、M P E G - 7 等の形式で著作権情報としてコンテンツ鍵生成条件などが記載された電子データを指定入力するようにしてもよい。

#### 【0 1 0 7】

暗号化コンテンツ生成部 1 2 1 は、入力されたコンテンツ鍵生成条件の内容を解析し（S 1 2 1 - 7）、コンテンツ鍵生成条件を抽出して（S 1 2 1 - 8）、オペレータ等の確認の上（S 1 2 1 - 9）、指定された条件に基づく暗号化コンテンツ C 1 の生成（S 1 2 1 - 1 0）及びコンテンツ鍵 K 1 の生成（S 1 2 1 - 1 1）を行う。

#### 【0 1 0 8】

暗号化コンテンツ発行部 1 2 2 は、暗号化コンテンツ C 1 が生成されたか否かの監視を行い（S 1 2 2 - 1、S 1 2 2 - 2）、暗号化コンテンツ C 1 が生成された場合には、予め指定されている、あるいは、暗号化の都度指定される暗号化

コンテンツ蓄積部（図 2 ではコンテンツ配信制御装置 1 4 0 の C 2）を検出し（S 1 2 2 - 3）、この蓄積部に暗号化コンテンツ C 1 を発行する（S 1 2 2 - 4）。

#### 【0 1 0 9】

コンテンツ鍵発行部 1 2 3 は、コンテンツ鍵 K 1 が生成されたか否かの監視を行い（S 1 2 3 - 1、S 1 2 3 - 2）、コンテンツ鍵 K 1 が生成された場合には、予め指定されている、あるいは、コンテンツ鍵生成の都度指定されるコンテンツ鍵蓄積部（図 2 では暗号化コンテンツ鍵制御装置 1 3 0 の K 2）を検出し（S 1 2 3 - 3）、この蓄積部にコンテンツ鍵を発行する（S 1 2 3 - 4）。

#### 【0 1 1 0】

暗号化コンテンツ鍵制御装置 1 3 0 は、装置固有鍵・媒体情報格納部 1 3 1、暗号化コンテンツ鍵生成部 1 3 2、コンテンツ鍵蓄積部 K 2、暗号化コンテンツ鍵蓄積部 K 3 を備え、図 6 に示す処理を実行する。

#### 【0 1 1 1】

図 6 において、まず暗号化コンテンツ制御装置 1 2 0 から、暗号化コンテンツ生成の都度、コンテンツ鍵発行部 1 2 3 にて発行されたコンテンツ鍵を受け付け（S 1 3 0 - 1）、コンテンツ鍵蓄積部 K 2 に複数蓄積する（S 1 3 0 - 2）。暗号化コンテンツ鍵生成部 1 3 2 は、コンテンツ識別情報と共に、媒体連携コンテンツ取得装置 2 2 0 の情報記憶媒体連携部 2 2 1 から情報記憶媒体 2 3 0 の媒体情報（媒体鍵情報及び媒体固有識別子）を通信回線 3 0 0 及びコンテンツ配信連携制御部 1 4 2 を経由して受け付け（S 1 3 2 - 1）、コンテンツ識別情報を基にコンテンツ鍵蓄積部 K 2 から暗号化コンテンツに対するコンテンツ鍵を選択し（S 1 3 2 - 2）、そのコンテンツ鍵を装置固有鍵・媒体情報格納部 1 3 1 に格納された装置固有鍵情報及び情報記憶媒体 2 3 0 の媒体情報を基に暗号化コンテンツ鍵 K 3 を生成し（S 1 3 2 - 7）、コンテンツ配信連携制御部 1 4 2 に発行する（S 1 3 2 - 8）。装置固有鍵・媒体情報格納部 1 3 1 には、予め全ての鍵情報を格納するようにしてもよいが、ユーザ側装置 2 0 0 からコンテンツ要求の都度、媒体情報と共に装置固有鍵を送ってもらうようにしてもよい。

#### 【0 1 1 2】

また、暗号化コンテンツ鍵生成部 1 3 2 は、オプション情報として暗号化コンテンツ鍵へのインクリメント指定がされているか判断する（S 1 3 2 - 3）。インクリメント指定がある場合には、暗号化コンテンツ鍵を生成する際、オプション情報（コンテンツ配信制御装置 1 4 0 を識別するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などを受け付け（S 1 3 2 - 4）、そのオプション情報を解析し（S 1 3 2 - 5）、インクリメント情報を生成する（S 1 3 2 - 6）。これらの情報の一部、条件として含んだ形で暗号化コンテンツ鍵を生成して（S 1 3 2 - 7）、コンテンツ配信連携制御部 1 4 2 に対して発行する（S 1 3 2 - 8）。

#### 【0 1 1 3】

ここで、情報記憶媒体 2 3 0 の媒体情報、コンテンツ配信制御装置 1 4 0 を識別するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報などは、コンテンツ配信連携制御部 1 4 2 を介して受け渡される以外に、媒体連携コンテンツ取得装置 2 2 0 などその他の装置あるいは直接入力などの手段で直接取得可能な場合もある。この場合でも、要求元に対して暗号化コンテンツ鍵を生成して発行する。

#### 【0 1 1 4】

コンテンツ配信制御装置 1 4 0 は、情報記憶媒体連携部起動情報生成部 1 4 1 と、コンテンツ配信連携制御部 1 4 2 と、コンテンツ視聴条件制御部 1 4 3 と、紐付け・暗号化処理部 1 4 4 と、暗号化コンテンツ蓄積部 C 2 と、暗号化オプション情報蓄積部 F 4 と、実績情報蓄積部 F 5 から構成され、図 7 に示す処理を実行する。

#### 【0 1 1 5】

図 7 において、コンテンツ配信制御装置 1 4 0 は、暗号化コンテンツ制御装置

1 2 0 にて暗号化され、暗号化コンテンツ発行部 1 2 2 にて発行された暗号化コンテンツを受け付けて暗号化コンテンツ蓄積部 C 2 に複数蓄積し（S 1 4 0 - 1 , S 1 4 0 - 2）、課金・決済部 1 1 5 にて発行されたユーザの選択コンテンツ情報とユーザ情報（コンテンツ視聴条件等）を受け付け（S 1 4 0 - 3）、ユーザ側装置 2 0 0 及び情報記憶媒体 2 3 0 と連携し、暗号化されたコンテンツ及び暗号化コンテンツ鍵等を配信する（S 1 4 0 - 4）。

#### 【0 1 1 6】

ここで、ユーザ側装置 2 0 0 及び情報記憶媒体 2 3 0 と連携するにあたって、情報漏洩対策からユーザ側装置 2 0 0 に搭載された連携アプリケーションが暗号化されている場合には、起動にあたって起動情報などが必要となる。そこで、情報記憶媒体連携部起動情報生成部 1 4 1 は、ユーザ管理制御装置 1 1 0 にてログイン時に生成された認証情報、ユーザ管理制御装置 1 1 0 にて蓄積されているユーザ情報（S 1 4 1 - 1 , S 1 4 1 - 2）、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体（ICカード等）2 7 0、ユーザアクセス・コンテンツ選択装置 2 1 0 に保管されたユーザを特定する識別子あるいは機器を特定するための識別子（S 1 4 1 - 1 , S 1 4 1 - 3）などを基に起動情報を生成し（S 1 4 1 - 5）、発行する（S 1 4 1 - 6）。

#### 【0 1 1 7】

コンテンツ配信連携制御部 1 4 2 は、暗号化コンテンツ及び暗号化コンテンツ鍵等を取得すると（S 1 4 2 - 1）、ユーザ側装置 2 0 0 及び情報記憶媒体 2 3 0 と連携し、暗号化コンテンツ及び暗号化コンテンツ鍵等の配信を行う。配信にあたって、ユーザ側装置 2 0 0 に対し、レスポンス要求（pingコマンド等のレスポンスを利用し、通信回線の状況把握をしてもよい）を行い（S 1 4 2 - 2）、ユーザ側装置 2 0 0 からのレスポンスを取得して（S 1 4 2 - 3）、その応答時間、到達経路情報を解析する（S 1 4 2 - 3）ことにより通信回線の負荷を把握する。

#### 【0 1 1 8】

コンテンツ配信連携制御部 1 4 2 は、上記のステップ S 1 4 2 - 2 ～ S 1 4 2 - 4 の処理を繰り返し、実績情報格納部 F 5 から過去の実績情報を取得して（S

1 4 2 - 5)、ユーザ側装置 2 0 0 に配信可能な通信回線の中から、応答時間が早く、到達経路情報により悪影響が予想される経路がなく、経路的に簡素化されている通信回線を判定し、一番妥当な通信回線として選択する (S 1 4 2 - 6)。さらに、選択したコンテンツの容量と解析された通信回線負荷等の情報からコンテンツの配信が終了するまでの想定時間を算出し (S 1 4 2 - 7)、この情報をユーザに発行して (S 1 4 2 - 8)、配信を行うかの確認を行う (S 1 4 2 - 9)。

#### 【0 1 1 9】

コンテンツ配信連携制御部 1 4 2 は、ユーザからの配信を行う旨の確認を受け付け、コンテンツ配信を開始する。また、配信を行わない旨の確認を受け付けた場合、配信指定通知を行い (S 1 4 2 - 1 0)、最終的に何時までにコンテンツ配信を終了させたいか等の予約配信の指定を可能にし (S 1 4 2 - 1 1)、候補を複数選出し (S 1 4 2 - 1 2)、現在の時間に近い順で配信指示を行い (S 1 4 2 - 1 3)、コンテンツ配信を開始する。

#### 【0 1 2 0】

コンテンツ視聴条件制御部 1 4 3 は、ユーザが選択したコンテンツ情報、ユーザ情報をユーザ情報蓄積部 F 1 から取得 (S 1 4 3 - 1)、あるいはコンテンツ配信連携制御部 1 4 2 からユーザが選択したコンテンツ情報、暗号化コンテンツ鍵識別子及び鍵情報を受け付け (S 1 4 3 - 2)、コンテンツ視聴条件 (視聴期間が制限されたコンテンツであることを示す情報、視聴可能日時 (期限) 情報、情報記憶媒体への書込制限情報、コンテンツ保護情報、年齢制限情報、バリアフリー対応情報 (手話種別・識別情報等) 等) を取得する (S 1 4 3 - 3)。このとき、受付／取得した情報中に暗号化が必要である旨の情報があるか判断し (S 1 4 3 - 4)、その情報がある場合には、鍵情報をもとに暗号化を行い (S 1 4 3 - 5)、暗号化コンテンツ視聴条件として発行する (S 5 3 0 - 6)。暗号化が不必要な場合、コンテンツ視聴条件として発行する (S 1 4 3 - 7)。

#### 【0 1 2 1】

紐付け・暗号化処理部 1 4 4 は、コンテンツ配信連携制御部 1 4 2 からユーザが選択したコンテンツ情報、暗号化コンテンツ鍵識別子及び鍵情報を受け付け、



コンテンツ配信制御装置 1 4 0 を識別するための情報、ユーザ側装置 2 0 0 の媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツ制御付随情報、ガイダンス情報などのオプション情報を受け付け（S 1 4 4 - 1）、暗号化コンテンツ及び暗号化コンテンツ鍵と紐付けして紐付け情報を生成し（S 1 4 4 - 2）、鍵情報をもとにオプション情報の暗号化を行い（S 1 4 4 - 3）、暗号化オプション情報 F 4 として発行する（S 1 4 4 - 4）。

#### 【0 1 2 2】

オプション情報入力装置 1 5 0 は、上記オプション情報をオペレータ等の入力操作によって暗号化コンテンツ鍵生成部 1 3 2 及び紐付け・暗号化処理部 1 4 4 に発行する。

#### 【0 1 2 3】

サーバ日時同期装置 1 6 0 は、サーバ日時同期部 1 6 1 を備える。このサーバ日時同期部 1 6 1 は、図 8 に示すように、WWWなどで公開されている公知の日時発行装置等から通信回線を利用して正確な日時を管理者が設定した時間間隔にて取得し（S 1 6 1 - 1, S 1 6 1 - 2）、日時発行要求を受け付け（S 1 6 1 - 3）、その要求に応じて保持している日時を要求元に発行する（S 1 6 1 - 4）。

#### 【0 1 2 4】

（ユーザ側装置 2 0 0）

ユーザアクセス・コンテンツ選択装置 2 1 0 は、ユーザが通信回線を利用してサービス加入申請、認証条件取得、ログイン、認証情報取得、コンテンツリスト表示要求、コンテンツリスト表示・閲覧、コンテンツ選択、与信情報取得、購入確認に至る、コンテンツ配信サービスを受け付けるための一連の手続きを実現するマンマシン・インターフェースと通信インターフェースを有する装置であり、例えば、パソコン、セットトップボックス、A V 機器、家電機器等、通信回線を介してサービスとの連携を可能にする装置である。その処理内容については、図 3 及び図 4 に示したユーザ管理制御装置 1 1 0 の処理内容の部分で既に説明したので、ここでは割愛する。

**【0 1 2 5】**

媒体連携コンテンツ取得装置 2 2 0 は、情報記憶媒体連携部 2 2 1 と、スタンドアロン起動情報生成部 2 2 2 と、正常書込確認部 2 2 3 と、コンテンツ視聴条件処理部 2 2 4 とから構成され、ユーザ側装置 2 0 0 に搭載あるいは接続される。各ブロック 2 2 1 ～ 2 2 4 の処理内容を図 9 及び図 1 0 に示す。

**【0 1 2 6】**

情報記憶媒体連携部 2 2 1 は、ユーザアクセス・コンテンツ選択装置 2 1 0、コンテンツ配信制御装置 1 4 0、あるいはユーザ自身からの起動要求を受け付け（S 2 2 1 - 1）、この起動要求に従い、ユーザ管理制御装置 1 1 0 にてログイン時に生成された認証情報、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体 2 7 0 あるいはユーザアクセス・コンテンツ選択装置 2 1 0 に保管されたユーザを特定する識別子、ユーザ側装置 2 0 0 を特定するための識別子などの情報を取得する（S 2 2 1 - 2）。ここで、通信回線 3 0 0 を介して起動情報を取得するか判断し（S 2 2 1 - 3）、通信回線 3 0 0 を介する場合には取得した媒体情報をコンテンツ配信制御装置 1 4 0 の情報記憶媒体連携部起動情報生成部 1 4 1 に発行し（S 2 2 1 - 4）、当該起動情報生成部 1 4 1 から起動情報を取得する（S 2 2 1 - 5）。

**【0 1 2 7】**

通信回線を利用していないスタンドアロン状態などにおいては、ユーザ管理制御装置 1 1 0 にてログイン時に生成された認証情報、ユーザ側装置 2 0 0 に搭載あるいは接続された記憶媒体 2 7 0 あるいはユーザアクセス・コンテンツ選択装置 2 1 0 に保管されたユーザを特定する識別子、ユーザ側装置 2 0 0 を特定するための識別子などの情報をスタンドアロン起動情報生成部 2 2 2 に発行する（S 2 2 1 - 6）。スタンドアロン起動情報生成部 2 2 2 は、起動情報生成条件を判断し（S 2 2 2 - 1）、条件に合致した状況にある場合には起動情報を生成し（S 2 2 2 - 2）、情報記憶媒体連携部 2 2 1 に発行する（S 2 2 2 - 3）。これにより、情報記憶媒体連携部 2 2 1 は、スタンドアロン起動情報生成部 2 2 2 から起動情報を取得する（S 2 2 1 - 7）。

**【0 1 2 8】**

続いて起動情報を用いて暗号化された連携アプリケーションを復号して処理を起動させ（S 2 2 1 - 8）、暗号化コンテンツ及び暗号化コンテンツ鍵等を取得するべく、情報記憶媒体 2 3 0 の媒体情報（情報記憶媒体の読込専用領域に書き込まれている媒体鍵情報及び媒体固有識別子）を取得し（S 2 2 1 - 9）、コンテンツ配信制御装置 1 4 0 に送付する（S 2 2 1 - 1 0）。さらに、端末日時同期装置 2 5 0 から日時情報を取得し（S 2 2 1 - 1 1）、コンテンツ配信連携制御部 1 4 1 と連携し、通信回線 3 0 0 を介してコンテンツ配信連携制御部 1 4 1 から送られてくる暗号化コンテンツと暗号化コンテンツ鍵等を受け付ける（S 2 2 1 - 1 2）。

### 【0 1 2 9】

ここで、情報記憶媒体連携部 2 2 1 は、コンテンツ配信連携制御部 1 4 2 から暗号化オプション情報 F 4 を受け付けた際には、起動情報を利用して復号化して（S 2 2 1 - 1 3, S 2 2 1 - 1 4, S 2 2 1 - 1 5）オプション情報を取得する（S 2 2 1 - 1 6）。そして、コンテンツ配信制御装置 1 4 0 を識別するための情報、媒体連携コンテンツ取得装置 2 2 0 を識別するための情報、地域を識別するための情報、ユーザを識別するための情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などを解析し（S 2 2 1 - 1 7）、この情報に基づくチェック（例えば、コンテンツ視聴条件内に視聴期間が記載されていた場合、その期間内であるか否か、あるいは、地域を識別する情報がある場合、指定の地域に該当しているか否か等）を行い（S 2 2 1 - 1 8）、これに準拠した形で動作制限等の制御（S 2 2 1 - 1 9）、ユーザ側装置 2 0 0 に搭載あるいは接続されたセキュリティが保たれた記憶媒体 2 7 0 の更新あるいは保管を行う（S 2 2 1 - 2 0）。さらに、必要に応じて暗号化コンテンツと暗号化コンテンツ鍵が書き込まれる情報記憶媒体 2 3 0 の書込可能領域に、指定されている情報をオプション情報として書き込む（S 2 2 1 - 2 1, S 2 2 1 - 2 2）。ステップ S 2 2 1 - 4 でオプション情報が得られない場合には、上記オプション情報があった場合の処理をスキップする。

**【0 1 3 0】**

続いて、取得した暗号化コンテンツ及び暗号化コンテンツ鍵を情報記憶媒体 2 3 0 に書き込むか判断し（S 2 2 1 - 2 1）、書き込み指示があった場合には情報記憶媒体 2 3 0 の書き込み可能領域に暗号化コンテンツ及び暗号化コンテンツ鍵を書き込む（S 2 2 1 - 2 2）。書き込み終了後、書き込み終了ステータスを発行し、正常書込確認部 2 2 3 に通知する（S 2 2 1 - 2 3）。ステップ S 2 2 1 - 2 1 で書き込み指示が得られなかった場合には、コンテンツの再選択を促す旨の通知を行う（S 2 2 1 - 2 4）。

**【0 1 3 1】**

正常書込確認部 2 2 3 は、情報記憶媒体連携部 2 2 1 からの書込終了ステータスを受け付け（S 2 2 3 - 1）、通信回線 3 0 0 を介して暗号化コンテンツ及び暗号化コンテンツ鍵等が全て正常に情報記憶媒体 2 3 0 の書込可能領域に書き込まれたかのチェックをサイズチェック、ベリファイ、実データ比較等により行い（S 2 2 3 - 2）、チェック終了後、端末日時同期装置 2 5 0 から日時情報を取得し（S 2 2 3 - 3）、書込正常終了時刻として課金・決済部 1 1 5 に発行する（S 2 2 3 - 4）。課金・決済部 1 1 5 はこれを受け、課金・決済情報蓄積部 F 3 の該当箇所を書込正常終了時刻を保管する。

**【0 1 3 2】**

コンテンツ視聴条件処理部 2 2 4 は、情報記憶媒体連携部 2 2 1 からユーザ情報等を取得し（S 2 2 4 - 1）、この情報をもとにユーザが選択しているコンテンツの情報（書込正常終了時刻等の状態を示す情報及び、視聴期間を示す情報等）が蓄積されているユーザ情報蓄積部 F 1、コンテンツ配信連携制御部 1 4 2 からコンテンツ視聴条件制御部 1 4 3 が取得、発信した暗号化コンテンツ視聴条件あるいはコンテンツ視聴条件等の情報を受け付け（S 2 2 4 - 2, S 2 2 4 - 3, S 2 2 4 - 4, S 2 2 4 - 5）、これを解析する（S 2 2 4 - 6）。

**【0 1 3 3】**

ここで、コンテンツ視聴条件が期間制限されたコンテンツ視聴タイプ、つまりコンテンツを一定期間のみ視聴可能とする条件付き視聴のタイプである場合、コンテンツ視聴タイプを示す情報と日時情報等を暗号化し（S 2 2 4 - 7, S 2 2

4-8)、情報記憶媒体連携部 2 2 1 に発行する (S 2 2 4-9)。情報記憶媒体連携部 2 2 1 は、これを受け付けて記憶媒体 2 7 0 に保管を行い (S 2 2 1-2 0)、暗号化コンテンツと暗号化コンテンツ鍵が書き込まれる情報記憶媒体 2 3 0 の書込可能領域に書き込む (S 2 2 1-2 1, S 2 2 1-2 2)。

#### 【0 1 3 4】

情報記録媒体 2 3 0 は、例えば DVD-RAM ディスクを利用する。このディスクには、読込専用領域に媒体鍵情報と媒体固有識別子が予め書き込まれている。書き込み可能領域には、媒体連携コンテンツ取得装置 2 2 0 との連携により、コンテンツ配信制御装置 1 4 0 から取得された暗号化コンテンツ、暗号化コンテンツ鍵、オプション情報、暗号化コンテンツ視聴条件が適宜書き込まれる。

#### 【0 1 3 5】

コンテンツ提示制御装置 2 4 0 は、コンテンツ提示処理部 2 4 1 と、装置固有鍵格納部 2 4 2 とから構成される。コンテンツ提示処理部 2 4 1 の処理内容を図 1 1 に示す。

#### 【0 1 3 6】

図 1 1 において、コンテンツ提示処理部 2 4 1 は、ユーザあるいはその他の装置、機能からの視聴要求を受け付け (S 2 4 1-1)、情報記憶媒体 2 3 0 内の読み出し専用領域に書き込まれている媒体情報及び書込可能領域に書き込まれている暗号化コンテンツ鍵を読み取ると共に、情報記憶媒体 2 3 0 または記憶媒体 2 7 0 に書き込まれているオプション情報、視聴条件、装置固有鍵格納部 2 4 2 にて保有する装置固有鍵を読み取る (S 2 4 1-2, S 2 4 1-3)。

#### 【0 1 3 7】

ここで、オプション情報の確認処理 (S 2 4 1-4, S 2 4 1-5) において、情報記憶媒体 2 3 0 または記憶媒体 2 7 0 にオプション情報がある場合には、このオプション情報を取得、解析して、その解析結果に基づく提示条件を発行する (S 2 4 1-6, S 2 4 1-7, S 2 4 1-8)。オプション情報がない場合には、ステップ S 2 4 1-6, S 2 4 1-7, S 2 4 1-8 をスキップする。

#### 【0 1 3 8】

続いて、視聴条件の存在を確認処理 (S 2 4 1-9, S 2 4 1-10) におい

て、視聴条件がある場合には、その視聴条件が暗号化されているか判断し（S 2 4 1 - 1 1）、暗号化されていない場合にはその条件を直接取得し、暗号化されている場合には暗号化視聴条件を取得すると共にオプション情報を取得し（S 2 4 1 - 1 3, S 2 4 1 - 1 4）、オプション情報に含まれる鍵情報に基づいて視聴条件を復号し取得する（S 2 4 1 - 1 5）。このようにして視聴条件が得られた場合には、その視聴条件を解析し（S 2 4 1 - 1 6）、その解析結果に基づいて端末日時同期装置 2 5 0 に日時情報発行要求を出し、同期装置 2 5 0 から要求に応じて発行される日時情報を取得する。視聴条件がない場合には、ステップ S 2 4 1 - 2 3 に移行する。

#### 【0 1 3 9】

次に、日限超過をチェックし（S 2 4 1 - 1 9, S 2 4 1 - 2 0）、超過している場合には、日限超過メッセージを発行してコンテンツを使用不能にする確認を行い（S 2 4 1 - 2 1）、情報記憶媒体 2 3 0 に書き込まれている情報を使用不能にする（S 2 4 1 - 2 2）。日限超過していない場合には、媒体情報、暗号化コンテンツ鍵、装置固有鍵をもとにコンテンツ鍵を生成し（S 2 4 1 - 2 3）、このコンテンツ鍵をもとに暗号化コンテンツを復号し（S 2 4 1 - 2 4）、提示可能として発行する（S 2 4 1 - 2 5）。

#### 【0 1 4 0】

端末日時同期装置 2 5 0 は、端末日時同期部 2 5 1 を備える。この端末日時同期部 2 5 1 は、図 1 2 に示すように、予め設定される時間間隔を取得し（S 2 5 1 - 1）、取得した時間間隔にて通信回線を介してサーバ日時同期部 1 6 1 から日時情報を取得し保持する（S 2 5 1 - 2）。また、媒体連携コンテンツ取得装置 2 2 0、コンテンツ提示制御装置 2 4 0 などから日時発行要求がある場合にはこれを受け付け（S 2 5 1 - 3）、最新日時を取得する必要があるときはサーバ日時同期部 1 6 1 から日時情報を取得し保持した上で（S 2 5 1 - 4, S 2 5 1 - 5）、保持している日時を発行する（S 2 5 1 - 6）。

#### 【0 1 4 1】

ここで、上記端末日時同期装置 2 5 0 は、ユーザ側装置 2 0 0 に搭載され、セット可能なタイマーとは異なり、外部から設定不可能な日時保持方式を有してい

る。

#### 【0 1 4 2】

コンテンツ視聴装置 2 6 0 は、ユーザがコンテンツ視聴を可能にする公知のディスプレイ、TV等の装置で、コンテンツ視聴制御部 2 6 1 とコンテンツ視聴部 2 6 2 とを備え、それぞれ図 1 3 に示す処理を実行する。まず、コンテンツ視聴制御部 2 6 1 は、コンテンツ提示処理部 2 4 1 で提示可能な状態となったコンテンツ等を受け付け（S 2 6 1 - 1）、視聴可能とする制御解析及び提示制御を行い（S 2 6 1 - 2, S 2 6 1 - 3）、コンテンツ視聴部 2 6 2 に発行する（S 2 6 1 - 4）。これを受けてコンテンツ視聴部 2 6 2 は、映像、音声等による視聴状態とする（S 2 6 2 - 1, S 2 6 2 - 2）。

#### 【0 1 4 3】

上記構成によるコンテンツ配信システムによれば、以下のような効果が得られる。

#### 【0 1 4 4】

（1）コンテンツの著作権保有者または著作権管理者からコンテンツ及びコンテンツ鍵生成条件を取得し、著作権保護された暗号化コンテンツ及びコンテンツ鍵を生成し、それらを発行可能にするようにしているので、著作権保有者または著作権管理者の要望に合わせてコンテンツの暗号化を図ることができる。

#### 【0 1 4 5】

（2）ユーザが通信回線を利用して著作権保護コンテンツ配信サービスを受けるにあたり、必要となる加入申請手続きを、著作権保護コンテンツ配信サービスを受けられる形態に合った形で提供するようにしているので、ユーザの加入申請手続きを簡略化しつつ、ユーザの利用環境に合わせて配信サービスを受けられるようにすることができる。

#### 【0 1 4 6】

（3）ユーザが著作権保護コンテンツ配信サービスを受けられるか判定し、この際、支払い方法がクレジットカードである場合、決済代行会社に対して必要な情報を発信し、決済代行会社から決済用識別子を受け取り、クレジットカード情報漏洩の危険性を回避するため不必要な情報は消去し、以降、決済用識別子を用

いて判定するようにしているので、不適格な利用者を排して、かつ安全な電子決済を実現することができる。

【0 1 4 7】

(4) 予め登録ユーザに認証条件を発行し、ユーザが通信回線を利用して著作権保護コンテンツ配信サービスにログインする際、認証条件の提示を行った上で著作権保護コンテンツ配信サービスを受けられる形態にしているので、適正ユーザのみがログイン可能となり、不適正ユーザの利用を排することができる。

【0 1 4 8】

(5) 発行された認証条件により著作権保護コンテンツ配信サービスにログインした際、どのようなサービスを受けられるユーザであるかを判定後、認証情報を発行するようにしているので、ユーザ毎にサービス内容を管理することができ、適切でかつきめ細やかなサービスを実現することができる。

【0 1 4 9】

(6) 発行された認証情報によりユーザあるいはユーザ側装置に見合ったコンテンツリストフォーマットを選択し、各種表示可能な形式等に生成し、発行するようにしているので、各ユーザのコンテンツ選択操作を簡単にすることができる。

【0 1 5 0】

(7) 発行されたコンテンツリストにより、ユーザによるコンテンツ選択を受け付け、決済用識別子をもとに決済代行会社に対して確認を行い、選択したコンテンツが購入可能か不可能かを通知するようにしているので、ユーザの過誤による不正購入を回避することができる。

【0 1 5 1】

(8) 暗号化されたコンテンツを複数蓄積し、ユーザが選択したコンテンツ情報とユーザ情報を受け付け、通信回線を介してユーザ側の情報記憶媒体と連携し、暗号化されたコンテンツ及び暗号化コンテンツ鍵等を通信回線を介して配信するようにしているので、適正ユーザへのみ暗号化コンテンツ及び暗号化コンテンツ鍵等の配信を行うことが可能となる。

【0 1 5 2】



(9) 情報記憶媒体の媒体情報（情報記憶媒体の読込専用領域に書き込まれている媒体鍵情報及び媒体固有識別子）を通信回線を介して送付し、通信回線を介して送られてくる暗号化コンテンツと暗号化コンテンツ鍵等を、媒体情報が書き込まれた情報記憶媒体または別の記憶媒体の書込可能領域に書き込むようにし、コンテンツに対して媒体情報に基づく暗号化がなされているので、媒体情報を持っていない状態での復号が不能となる。このため、たとえ暗号化コンテンツ及び暗号化コンテンツ鍵が複製されたとしても、媒体情報を持っていない、あるいは異なる媒体情報を持つユーザ側端末装置では、コンテンツ鍵の生成、暗号化コンテンツの復号ができず、これによって不正に複製されたコンテンツの視聴を制限することができる。

#### 【0 1 5 3】

(10) ユーザ側装置に搭載された著作権保護コンテンツ配信サービスを実現するための機能が暗号化されている場合、通信回線を介して各種情報を取得し、起動情報を生成、発行あるいは、通信回線を利用しないスタンドアロン状態などにおいては、独自に起動情報を生成し、起動させるようにしているので、登録された機器以外の装置でサービスを受けることができなくなり、不正利用を排することができる。

#### 【0 1 5 4】

(11) 著作権保護コンテンツ配信サービスにてコンテンツを配信する際、配信可能な通信回線で一番妥当な（負荷が少ない等）通信回線を選択し、コンテンツの配信が終了するまでの想定時間の情報を発行可能とし、コンテンツ配信を開始するようにしているので、ユーザ側の負担を軽減し、利用効率を向上させることができる。

#### 【0 1 5 5】

(12) 各種識別情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などのオプション情報を、暗号化コンテンツ及び暗号化コンテンツ鍵と紐付けし、必要に応じて暗号化を行い、暗号化オプショ

ン情報として通信回線を介して発行するようにしているので、ネットワーク上の情報の漏洩に対する問題を改善しつつ、ユーザにとってよりの確なコンテンツ配信サービスを行うことができる。

#### 【0 1 5 6】

(1 3) 最終的に何時までにコンテンツ配信を終了させたいか等の予約配信の指定を発行可能とし、候補を複数選出し、現在の時間に近い順あるいは、優先度指定によりコンテンツ配信を行うようにしているので、ユーザの利用時間の制約を排し、効率よく配信を行うことが可能となる。

#### 【0 1 5 7】

(1 4) コンテンツ視聴条件（視聴期間が制限されたコンテンツであることを示す情報、視聴可能日時（期限）情報、情報記憶媒体への書込制限情報、コンテンツ保護情報、年齢制限情報、バリアフリー対応情報（手話種別・識別情報等））を受け付け、必要に応じて暗号化を行い、発行するようにしているので、ユーザの要望または利用制限事項に合わせて適切な視聴制限を加えることが可能となる。

#### 【0 1 5 8】

(1 5) 公知の日時発行装置等から通信回線を利用して正確な日時を取得し、要求に応じて保持している日時を要求元に発行するようにし、ユーザ側の機器に搭載されたタイマーは、外部から設定不可能な日時保持方式を採用するか、あるいはセット可能なタイマーであっても、タイマーの日時を強制的に外部からサーバ側に同期して最新日時に更新されるようにすることで、ユーザ側で日時をずらして時間的な制限を外すような不正利用を未然に防ぐことができる。

#### 【0 1 5 9】

(1 6) 通信回線を介して配信された暗号化コンテンツ及び、暗号化コンテンツ鍵等が正常に情報記憶媒体の書込可能領域に書き込まれたかのチェックを行い、(1 5) のタイマーから日時情報を取得し、それら情報を著作権保護コンテンツ配信サービス提供側に発行するようにしているので、配信サービス提供者側で配信した情報の最終結果を確認することができ、適切な課金処理を実施することが可能となる。

**【0160】**

(17) (14) の暗号化オプション情報を受け付けた際には、(10) の起動情報を利用して復号化し、オプション情報を取得、各種識別情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などを解析し、この情報にもとづくチェックを行い、これに準拠した形で動作制限等の制御及び記憶情報の更新あるいは保管を行い、必要に応じて情報記憶媒体の書込可能領域にオプション指定情報を書き込むようにしているので、オプションの指定・処理を簡単かつ安全に実施することが可能となる。

**【0161】**

(18) 情報記憶媒体への書込み処理を行う際、コンテンツ視聴条件が期間制限されたコンテンツ視聴タイプつまりコンテンツを一定期間のみ視聴可能とする条件付き視聴のタイプである場合、コンテンツ視聴タイプを示す情報と日時情報を暗号化し、ユーザ側装置の記憶媒体に保管するか、あるいは、暗号化コンテンツと暗号化コンテンツ鍵が書き込まれる情報記憶媒体の書込可能領域に書き込むようにしているので、条件に合致しない状態となったときに視聴できないようにすることができ、著作権保護をいっそう高めることができる。

**【0162】**

(19) コンテンツ識別情報をもとに暗号化コンテンツに対するコンテンツ鍵を選択し、発行するようにしているので、他の暗号化コンテンツがあってもこれを視聴することができないようにすることが可能となる。

**【0163】**

(20) 暗号化コンテンツ鍵は、通信回線を介して情報記憶媒体の情報（情報記憶媒体の読込専用領域に書き込まれている媒体鍵情報及び媒体固有識別子）により生成される他、各種識別情報、コンテンツ視聴条件を示す情報、コンテンツの制御付随情報（例えば、メニュー情報、コンテンツ内の遷移情報（サムネイル、メニューリンク等）、外部リンク情報（インターネットへの接続アドレス等）、ガイダンス情報（文字、静止画等）等）などの情報を含んだ形で生成するよう

にしているので、他の情報記録媒体への書き込み、他の装置による視聴処理を排することが可能となる。

#### 【0 1 6 4】

(2 1) ユーザ等からの視聴要求を受け付け、情報記憶媒体内の情報を読み取り、ユーザ側装置にて保有する装置固有鍵情報と、情報記憶媒体の媒体情報（情報記憶媒体の読込専用領域に書き込まれている媒体鍵情報及び、媒体固有識別子）と、情報記憶媒体の書込可能領域に書き込まれている暗号化コンテンツ鍵をもとにコンテンツ鍵を生成し、このコンテンツ鍵をもとに暗号化コンテンツを復号し提示可能とするようにしているので、他の媒体への不正な複製による利用をしたとしても、コンテンツ鍵の生成及びコンテンツの復号を行うことができず、その視聴を排することができる。また、他の装置で利用しようとしても、装置固有鍵情報が得られないため、同じくコンテンツ鍵の生成及びコンテンツの復号を行うことができず、その視聴を排することができる。

#### 【0 1 6 5】

(2 2) ユーザ側装置の記憶媒体あるいは情報記憶媒体にオプション情報がある場合、これを読み込み、この情報にもとづく提示処理を行うようにしているので、サービス配信者側及びユーザ側双方で任意のオプション事項を選択することで多彩なサービスを享受することが可能となる。

#### 【0 1 6 6】

(2 3) ユーザ側装置の記憶媒体あるいは情報記憶媒体に視聴条件がある場合、これを読み込み、(1 5) のタイマーから日時情報を取得し、蓄積されているコンテンツが期間を超過しているかのチェックを行い、超過している場合はユーザに対してこの旨を通知し、コンテンツを使用不能にするようにしているので、例えばコンテンツのレンタルのように日限による管理を要する場合に対応することが可能となる。

#### 【0 1 6 7】

#### 【発明の効果】

以上述べたように本発明によれば、コンテンツの不正流通を阻止する著作権保護の仕組みを具備した形で、コンテンツの著作権保有者または著作権管理者から

信頼を得ることにより、リーズナブル価格で通信回線を利用した有効なコンテンツの配信サービスを実現することのできるコンテンツ配信サービス提供装置とそのサービスを受ける端末装置を提供することができる。

【図面の簡単な説明】

【図 1】 本発明に係るコンテンツ配信システムの一実施形態の構成を示す概念図。

【図 2】 上記実施形態のコンテンツ配信システムにおける具体的な構成を示すブロック図。

【図 3】 上記実施形態のユーザ管理制御装置の処理内容を示すフローチャート。

【図 4】 上記実施形態のユーザ管理制御装置の処理内容を示すフローチャート。

【図 5】 上記実施形態の暗号化コンテンツ制御装置の処理内容を示すフローチャート。

【図 6】 上記実施形態の暗号化コンテンツ鍵制御装置の処理内容を示すフローチャート。

【図 7】 上記実施形態のコンテンツ配信制御装置の処理内容を示すフローチャート。

【図 8】 上記実施形態のサーバ日時同期装置の処理内容を示すフローチャート。

【図 9】 上記実施形態の媒体連携コンテンツ取得装置の処理内容を示すフローチャート。

【図 10】 上記実施形態の媒体連携コンテンツ取得装置の処理内容を示すフローチャート。

【図 11】 上記実施形態のコンテンツ提示制御装置の処理内容を示すフローチャート。

【図 12】 上記実施形態の端末日時同期装置の処理内容を示すフローチャート。

【図 13】 上記実施形態のコンテンツ視聴装置の処理内容を示すフローチャート。

ャート。

【符号の説明】

110…ユーザ管理制御装置、111…ユーザ管理部、112…決済代行処理部、113…ユーザ認証部、114…コンテンツリスト表示・選択部、115…課金・決済部、

120…暗号化コンテンツ制御装置、121…暗号化コンテンツ生成部、122…暗号化コンテンツ発行部、123…コンテンツ鍵発行部、

130…暗号化コンテンツ鍵制御装置、131…装置固有鍵・媒体情報格納部、132…暗号化コンテンツ鍵生成部、

140…コンテンツ配信制御装置、141…情報記憶媒体連携部起動情報生成部、142…コンテンツ配信連携制御部、143…コンテンツ視聴条件制御部、144…紐付け・暗号化处理部、

150…オプション情報入力装置、160…サーバ日時同期装置、161…サーバ日時同期部、

210…ユーザアクセス・コンテンツ選択装置、

220…媒体連携コンテンツ取得装置、221…情報記憶媒体連携部、222…スタンドアロン起動情報生成部、223…正常書込確認部、224…コンテンツ視聴条件処理部、

230…情報記憶媒体、

240…コンテンツ提示制御装置、241…コンテンツ提示処理部、242…装置固有鍵格納部、

250…端末日時同期装置、251…端末日時同期部、

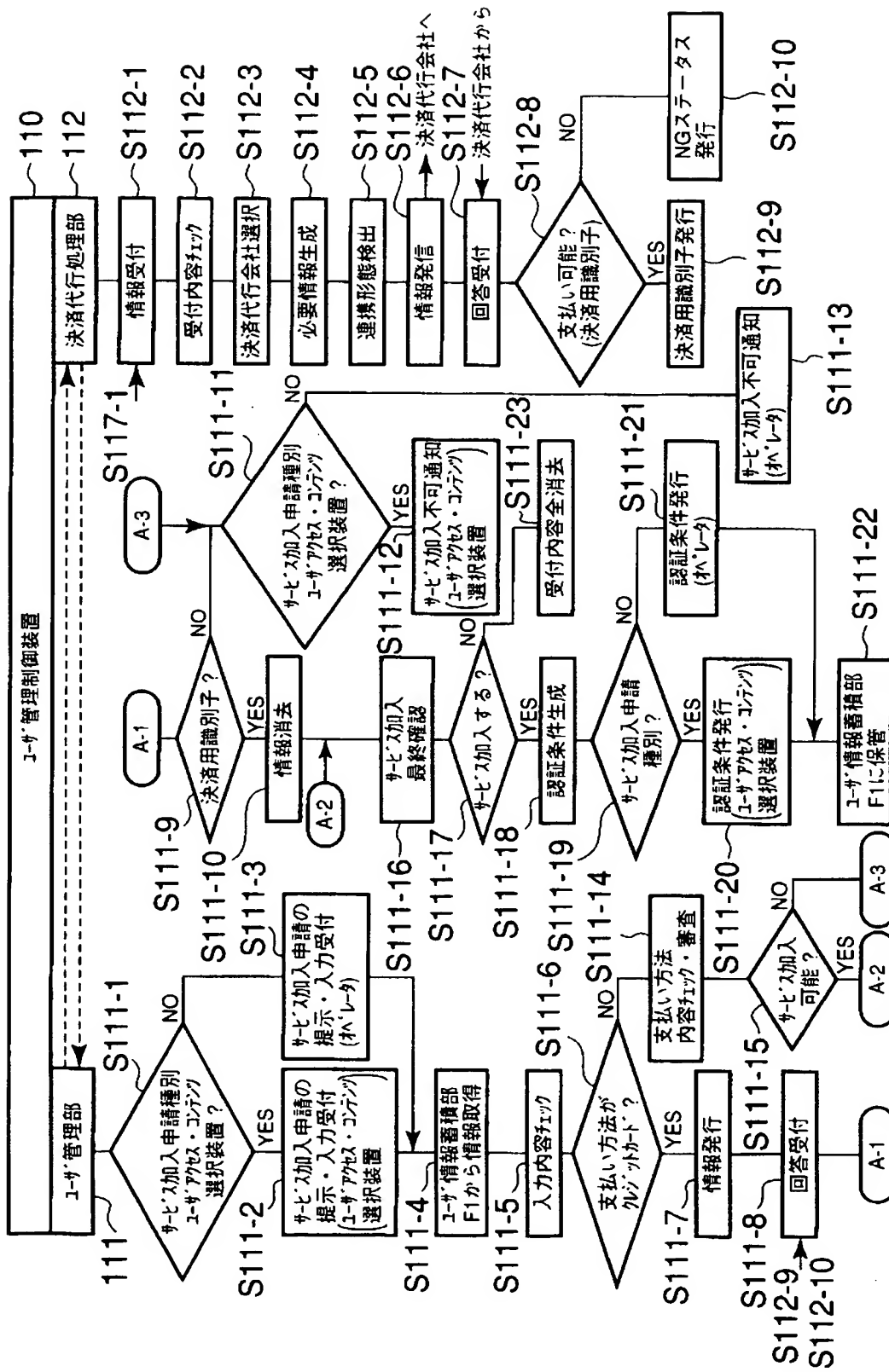
260…コンテンツ視聴装置、261…コンテンツ視聴制御部、262…コンテンツ視聴部。



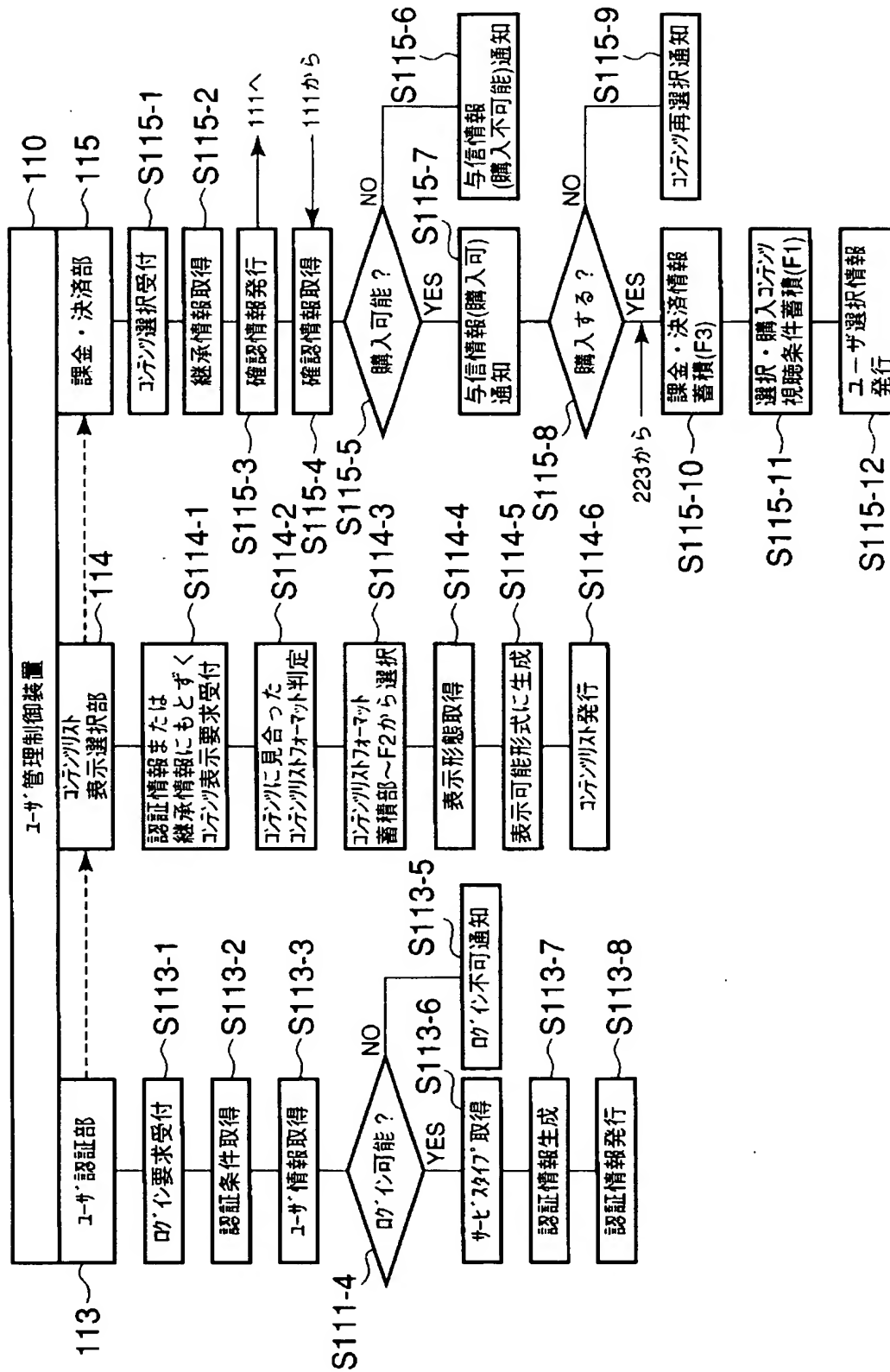




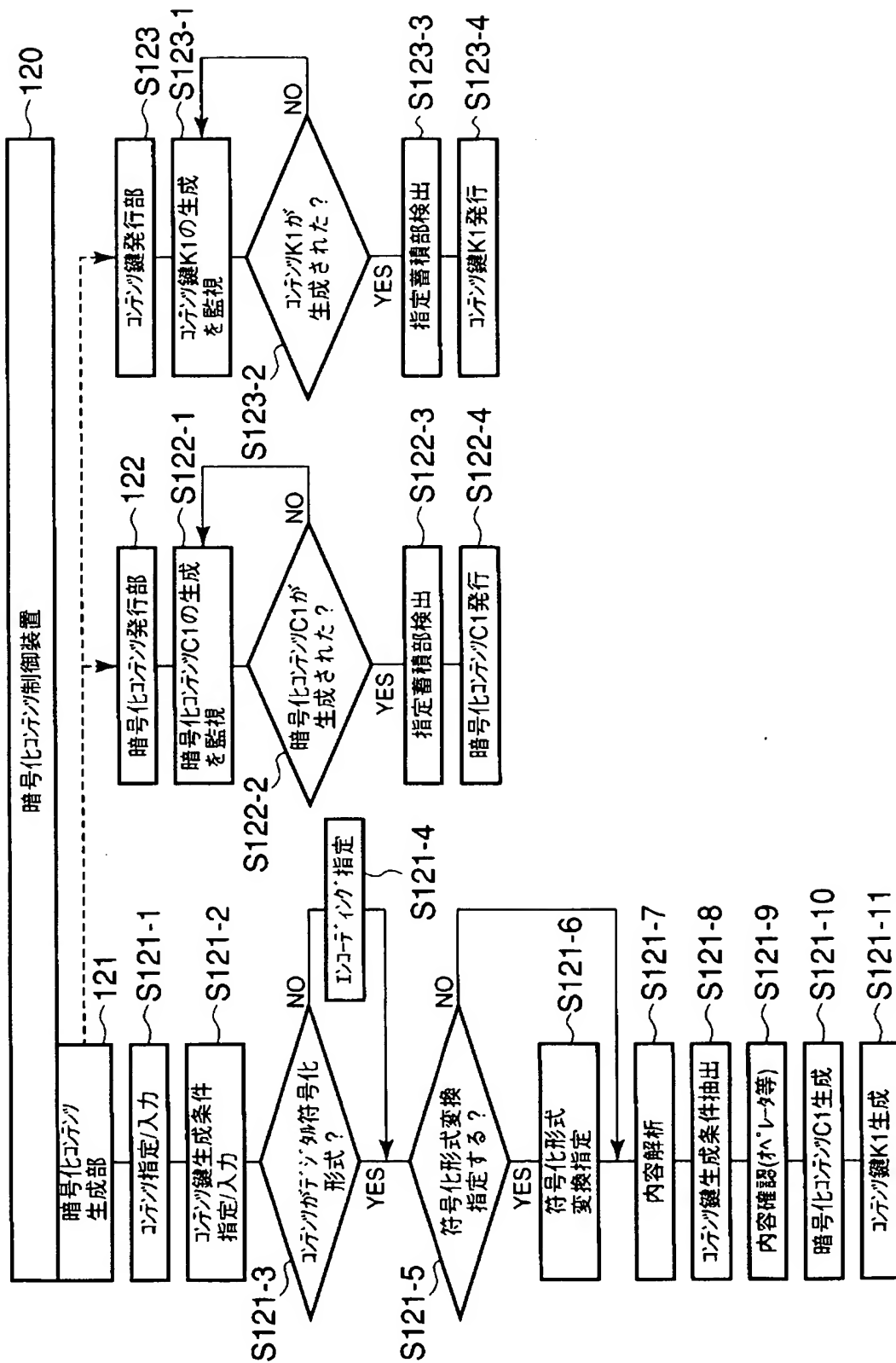
【図 3】



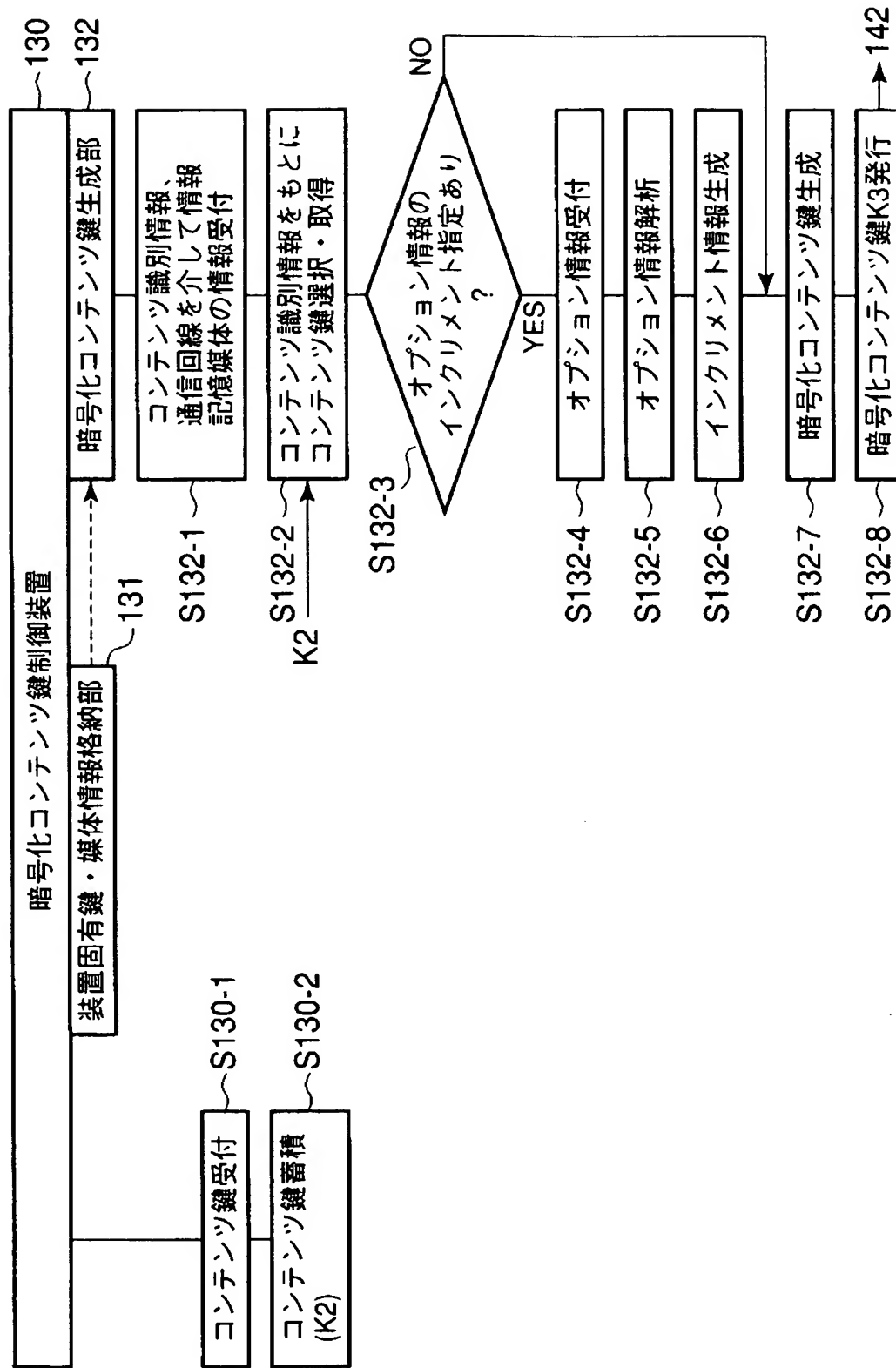
【図4】



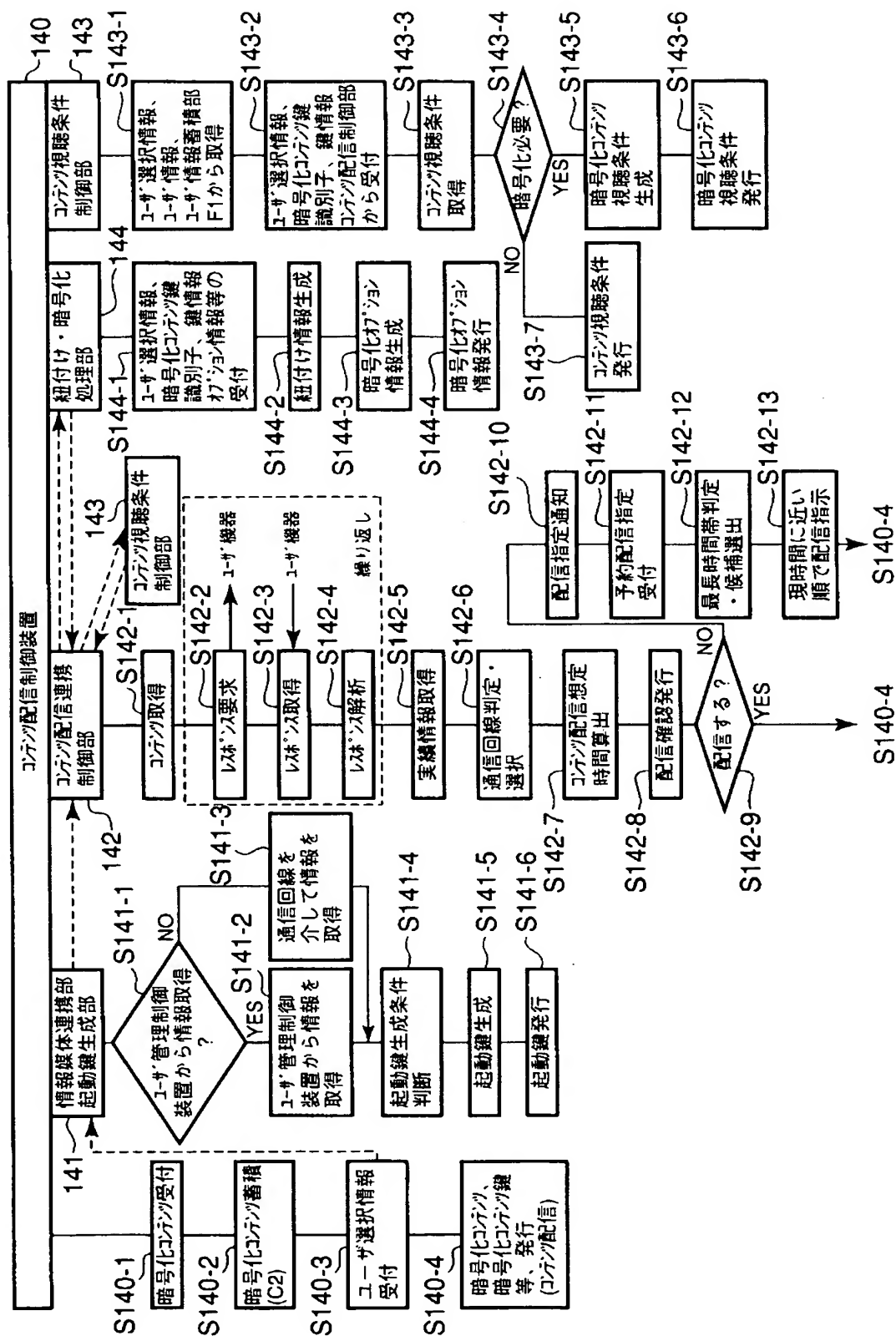
【図 5】



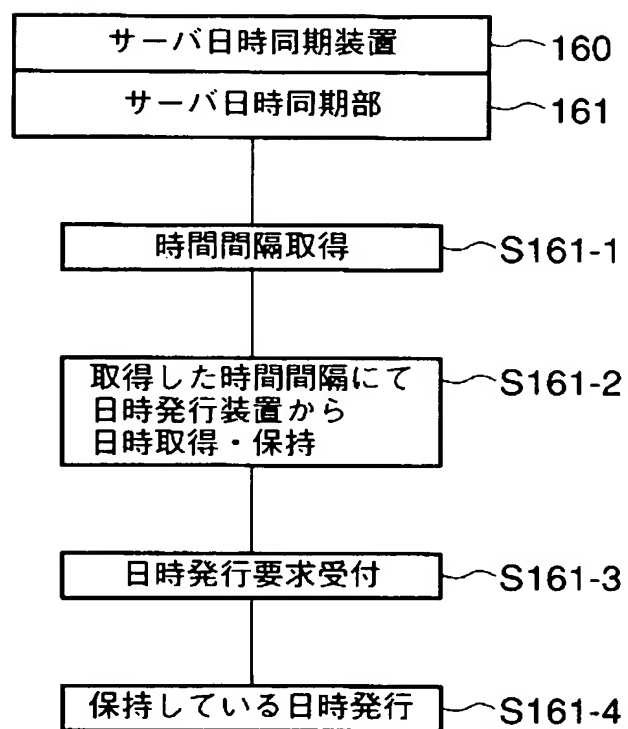
【図 6】



【図 7】

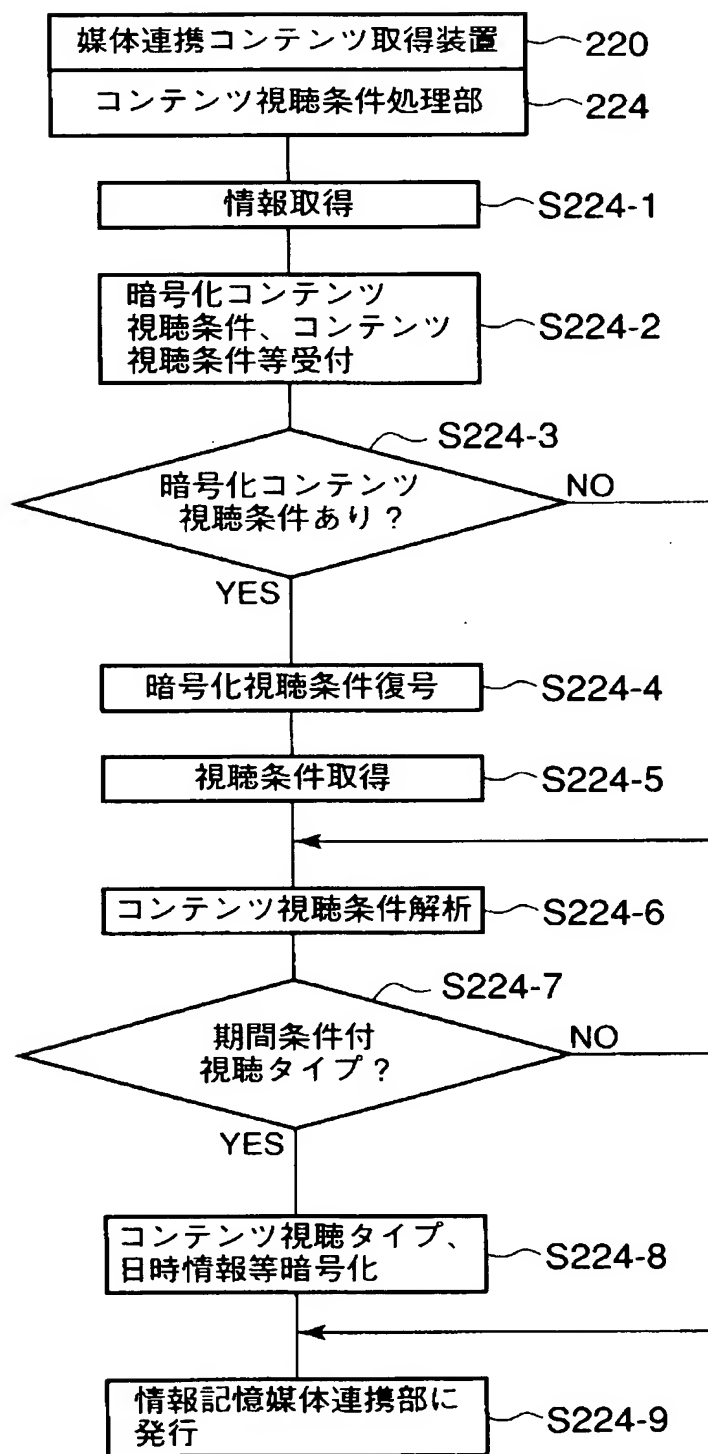


【図 8】



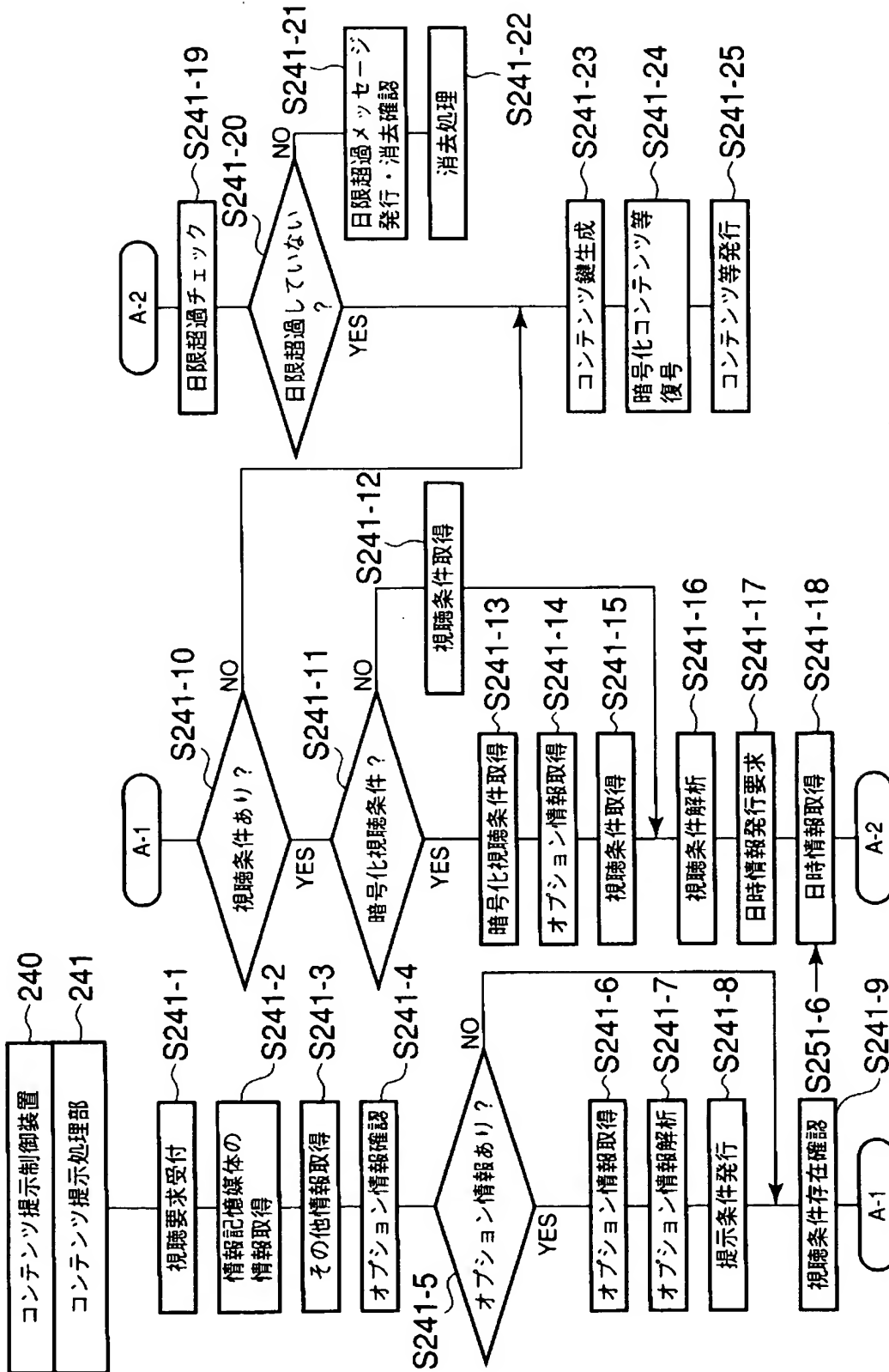


【図 10】

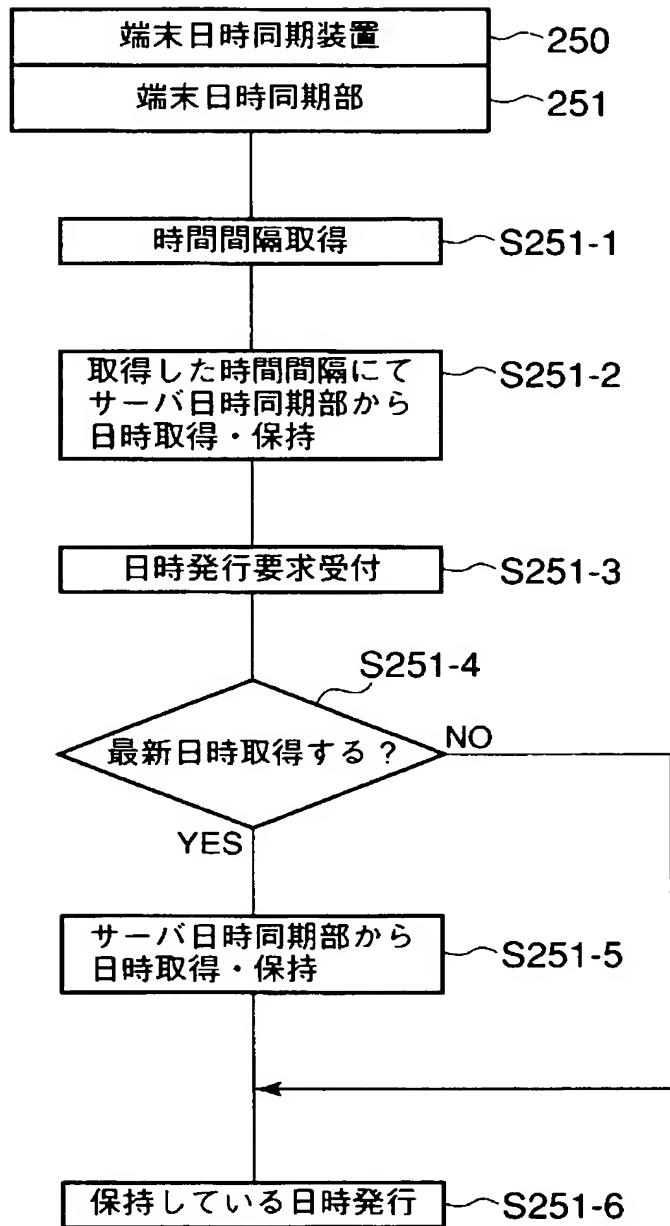




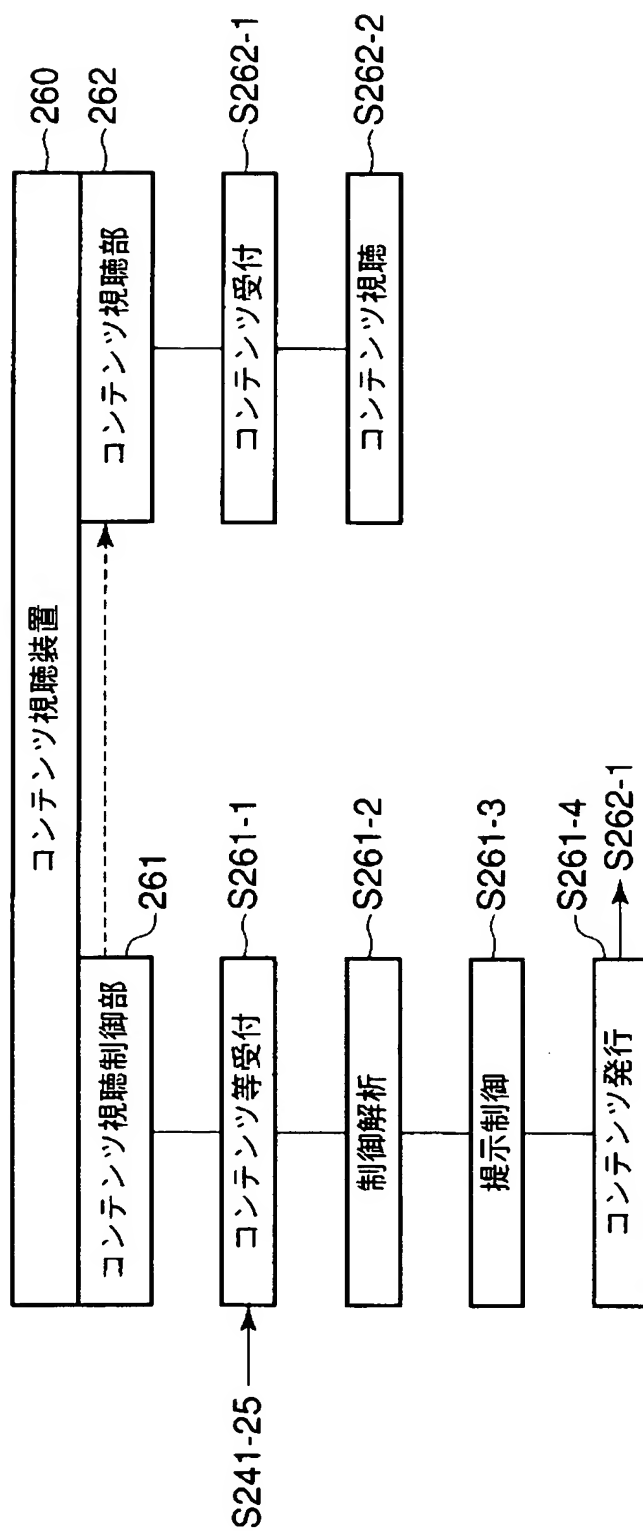
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 通信回線を利用し、コンテンツの不正流通を阻止する著作権保護の仕組みを具備したコンテンツの配信サービスを実現する。

【解決手段】 コンテンツ配信側において、ユーザ管理制御装置 1 1 0 にて、ユーザ毎にサービス提供時の認証情報及び配信リストの配布、コンテンツ選択要求受付、課金・決済を管理する。一方、暗号化コンテンツ制御装置 1 2 0 にて、著作権保有者または著作権管理者からのコンテンツ鍵生成条件を基にコンテンツ鍵及びこのコンテンツ鍵による暗号化コンテンツを生成し、暗号化コンテンツ鍵制御装置 1 3 0 にて、コンテンツ要求時に提示される媒体情報を用いて該当コンテンツ鍵を暗号化して要求元に配信し、コンテンツ制御配信装置 1 4 0 にて、コンテンツ要求時に該当する暗号化コンテンツを要求元に配信する。

【選択図】 図 1

特願 2 0 0 3 - 1 4 6 7 0 4

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 3 0 7 8 ]

1. 変更年月日	2 0 0 1 年 7 月 2 日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目 1 番 1 号
氏 名	株式会社東芝